CHAPTER 1

INTRODUCTION

With the advancements in the technology the communication between the two parties has witnessed the security distortion tremendously in recent years. The communication involves the exchange of the data consisting of textual documents, images and video files. To provide copy protection and copyright protection for digital audio and video data, two complementary techniques are being developed: encryption and watermarking. The encryption algorithms have been developed earlier for the transmission such information over the internet and other media safely. But these algorithms have proved to be inefficient in providing complete security for data exchange. The generation of the keys for encrypting and decrypting the data has become time consuming. The storage of keys requires huge memory space and the transmission of such keys gets distorted with introduction of the intruders to the communication systems. Even after the receiver has received and decrypted the data, the data is not clear and no longer protected. The watermarking systems have been developed for better security of the data. Watermarking techniques can complement encryption by embedding a secret imperceptible signal, a watermark, directly into the clear data. In these techniques, the cover-image is used to hide the secret information and the stego-image is the cover- image with the secret data embedded inside. It hides the secret information in general files secretly first and then transmits these files through network, because they look the same as general files, they can escape from the attention of illegal interceptors easily and therefore the secret information is not easy to be attacked. A digital watermark is in fact a piece of information inserted and hidden in the media content. This information is imperceptible to a human observer but can be easily detected by a computer. The watermarking is well-suited for the protection of multimedia content. The watermark can be visible or invisible [1]. In visible watermarking, the information is visible in the video while in invisible

watermarking, information is not visible. It can be detected only by the owner [38]. Another classification of is based on domain which the watermark is applied i.e., the spatial or the frequency domain. The easiest way to watermark a video is to change directly the values of the pixels, in the spatial domain. A more advanced way to do it is to insert the watermark in the frequency domain [2][3].

1.1. DIGITAL WATERMARKING

A digital watermark is a type of code or image incorporated in a noise-tolerant signal such as audio or image data which is used to identify ownership of the copyright of that signal or content of the document for authentication. It is a process of hiding digital information in a carrier signal such that the hidden information does not need to contain a relation to the signal. Therefore, it is used to verify the authenticity or integrity of the signal or to show the identity of its owners. The properties of a digital watermark depend on the applications. In case of media files having copyright information, a digital watermark is robust against modification which is applied to the carrier signal [20].

The properties of a digital watermark are mentioned below:

1) A digital watermark is invisible perceptually to prevent obstruction of the original image.

2) A digital watermark is statistically invisible, therefore it cannot be detected or erased.

3) Watermark extraction is fairly simple such that the detection process requires very less amount of time for computation.

4) Watermark detection should be accurate in order to reduce false positives i.e., the detection of a non-marked image and false negatives i.e., the non-detection of a marked image.

5) A large number of watermarks can be produced in this process.

6) Watermark is robust in the case of filtering, additive noise, compression and other forms of image manipulation.

7) The watermark is able to identify the ownership of the image.

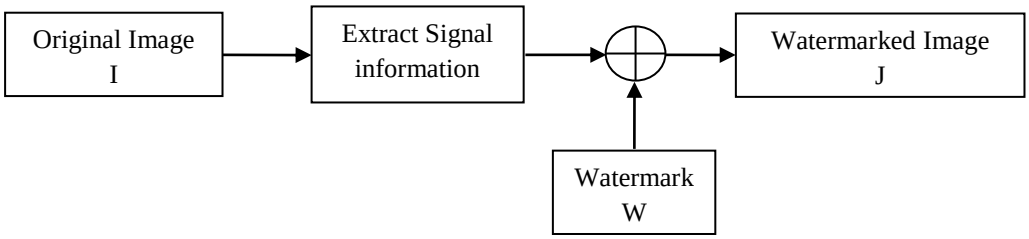

Fig1. Watermark Transmission

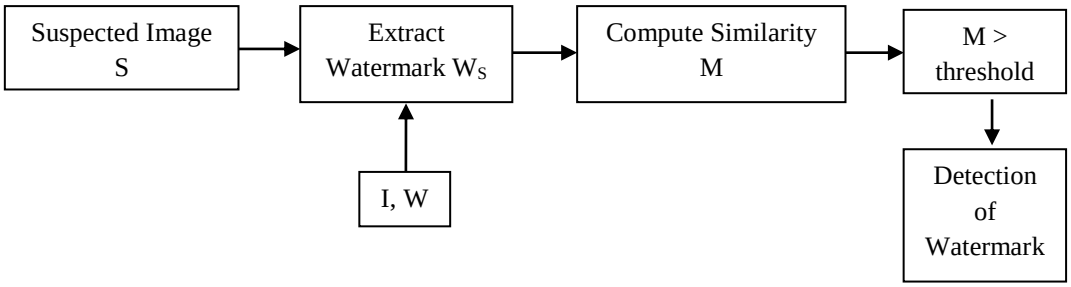

Fig2. Watermark Detection

The above figures show a general watermarking approach. Fig1. shows the watermark transmission. In this phase, the watermark W is generated as a pseudo-random sequence to ensure statistical invisibility. Signal information, such as DCT coefficients are extracted from the original image I and embedded into the information to form the watermarked image J.

In the watermark detection phase as shows in fig.2, a suspected image S is taken as input for obtaining its signal information. A suspected watermark WS is extracted based on knowledge of the original image I and the watermark W. A similarity measure M is calculated based on the values of WS and W, which is then compared with a threshold value. If the value of M is larger than the threshold value, then the watermark is detected.

1.1.1 Basic requirements of watermarking

Each watermarking application has its own specific requirements. Some of the general requirements are outlined here: [21]

1. Perceptual transparency: the watermarking algorithm must embed the watermark such that this does not affect the quality of the host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark [4]. The smallest modification in the host data may become apparent when the original data is compared directly with the watermarked data. Since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it may be sufficient that the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data [22].

2. Watermarking load: The amount of information that can be stored in a watermark depends on the application. The information should be embedded such that the pixel value of image does not leave the base value of the pixel.

3. Robustness: There should be no way in which the watermark can be removed or altered without sufficient degradation of the perceptual quality of the host data. If a watermark is used for another application, it is desirable that the watermark always remains in the host data, even if the quality of the host data is degraded, intentionally or unintentionally [19].

4. Security: A watermarking technique is secure if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark [21].

5. Blind detection scheme. Non-blind detection needs the original host signal, which is very inconvenient to use the original data, because of the huge video data. Blind detection does not need the original host image.

6. High real-time: Three-dimensional video signal has more the amount of data than the image does. So calculation quality is larger and embedding /detection needs more times. The procession of embedding, using video compression standard for these specific structures such as motion vector coding.

7. Random detection: The watermark is detected in any position of the video rather than the position according to the video playback order to detect the watermark.

The cryptography based security techniques provide assurance against data confidentiality, authenticity and integrity on transmission over the public channels. These techniques do not provide protection against unauthorized copying or transmitting of illegal materials. This leads to the need of watermarking for detection of copyright material and content authorization.

1.1.2 Application of Watermarking

1) Copyright protection: The owner of data can embed a watermark representing copyright information in his data. This watermark can prove his ownership in court when someone has infringed on his copyrights. The watermarking approaches applied for owner authentication or copyright protection, where an owner or producer identification is embedded to prove ownership or source of the cover. A recent approach to copyright protection is to use digital

watermarking to identify single copies of an original file by embedding a transaction code, a customer ID or a simple continuous number into each copy. Whenever a copy is found, the watermark can be retrieved and the source can be identified by the embedded individual information. Although the customer is free to use and consume the media data but if he passes the content into illegal environments and copies are found, then he can be identified. Therefore this application is called customer identification or customer tracing watermarking [18].

2) Fingerprinting: The owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties. Fingerprint is referred to as another application area as transaction tracking or traitor tracking is applied to track back illegal duplication and distribution of the content. Multimedia fingerprint is a way to prevent illegal redistribution of media content. Prior to distribution, each copy of the media document is uniquely embedded with an ID, known as digital fingerprint. When an unexpected copy is found, the embedded fingerprint can be extracted and used to track back to the source of leak. To escape from detection, attackers may employ various attacks to try to remove the fingerprints. Orthogonal fingerprinting is a typical example of non-coded fingerprinting where mutually orthogonal spreading sequences are assigned to users as fingerprint.

3) Medical application is another well-known domain to provide both authentication and confidentiality in a reverse manner without affecting the medical image.

4) Monitoring: By embedding watermarks in commercial advertisements an automated monitoring system can verify whether advertisements are broadcasted as contracted. Not only commercials but also valuable TV

products can be protected by broadcast monitoring. Watermarking can also be used to identify specific content in a broadcast monitoring system in which it is embedded to identify a cover in a broadcast channel to monitor its usage, for example for the automatic generation of song tracking lists. In this case, the requirements are similar to the copyright protection watermarking with respect to transparency and robustness. But in addition, a low complexity at watermarking detection is necessary to enable real-time monitoring on multiple channels.

5) Indexing: Indexing is used for indexing of video mail, where comments can be embedded in the video content where markers and comments can be inserted that can be used by search engines. The embedding of additional information into a cover or a set of covers is called annotation watermarking which is another approach. The annotation watermark only needs to be robust against a specified set of transformations which are known to occur in the application domain.

6) Data hiding: Watermarking techniques can be used for the transmission of secret private messages. This provides security of the data over the network from the unauthorized access and prevents from the attacks.

7) Integrity protection is another application domain where the watermark enables to verify the integrity of the cover in order to recognize manipulations and recover the original information after manipulations without the need to access the original cover. This can be achieved with or without knowledge of the content.

The video data have one more dimension time dimension than image data and successive similar frames are presented with very small time gap, visibility problem

in video watermarking. To prevent quality degradation in video caused by watermark embedding, more sophisticate watermarking scheme is needed.

In this thesis work, we have applied the PSO hybridized with the rough set theory for the selection of the optimal set of motion vectors. The algorithm tries to find the feature vectors by dividing the image into regions with boundary with the rough set theory. Each region is further optimized with the swarm based PSO algorithm.

1.2 LITERATURE REVIEW

The literature review has been divided into two groups demonstrating the research work done in the area of image as well as video watermarking in group I and some of the Swarm based Intelligent algorithms in group II.

In case of images, watermarking techniques are classified based on two working domains. Spatial Domain in which pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image and Frequency Domain in which values of certain frequencies change.

I. Watermarking Techniques

Watermarking techniques can be divided into four categories based on the type of document to be watermarked such as Text watermarking, Image watermarking, Audio watermarking and Video watermarking. In this thesis, we have a brief review of audio, image and video watermarking schemes [35].

1.2.1 Image Watermarking

Initially, watermarking method obtains a checksum of the image data and then embeds the checksum into the LSB of randomly chosen pixels. Others add a modified

maximal length linear shift register sequence to the pixel data which can identify the watermark by using spatial cross correlation function of the modified sequence and part of the watermarked image. Watermarks can modify the images spectral by modulating DCT, DFT or DWT coefficients according to a sequence known only to the owner. As a result, the security level of the watermark in the image increases while maintaining the imperceptibility of the mark.

1.2.1.1 Spatial domain

A watermarking method based on the spatial domain scatters information to be embedded to make the information more secure so that it is very difficult to detect. It uses minor change of the value of pixels. This approach has an advantage which is it is strong for cropping and translation.

Various approaches for spatial domain techniques have been proposed so far which are checksum techniques, two-dimensional spatial watermark, spread spectrum approach are some of them.

1.2.1.1.1 Checksum Technique

In this approach, a watermark is formed from the checksum value of the seven most significant bits of all pixels. A checksum is the modulo-2 addition of a sequence of fixed-length binary words which is a type of hash function. This technique randomly chooses the locations of the pixels that are to contain one bit of the checksum. The pixel locations of the checksum together with the checksum value form the watermark which must be kept secret. To verify the watermark, the checksum of a test image is obtained and compared to the watermark.

The advantages of this technique are mentioned below:

1. Embedding watermark only changes half of the pixels that covered by it, as a result it not only reduces visual distortion but also increases security.
2. An image may hold many watermark as long as they do not overlap.

The drawback of this technique is that it is fragile, therefore any change to either the image data or the embedded checksum can cause the verification procedure to fail.

1.2.1.1.2 Basic M-sequence approach

In this approach, the watermark is formed based on using a modified m-sequence. A linear feedback shift register with n stages can form pseudo-random binary sequences with maximum period of 2*n-1*. Two types of sequences may be formed from an m-sequence: unipolar and bipolar.

The advantages of this technique are that the watermark is robust to small amounts of noise, in the image. Successive watermarks treat the previously watermarked image as a new. An attacker can deduce watermark if 2n consecutive bits in it are known.

The drawback of this method is that it does not protect the DC value of the pixels covered by an individual block.

1.2.1.1.3 Secure Spread Spectrum Watermarking for Multimedia

This approach inserts a watermark into the spectral components of the data using the techniques which are analogous to spread spectrum communication, therefore hiding a narrow band signal in a wideband channel

The advantages of this approach are as

1. The watermark is difficult to remove for an attacker even when several individuals combine together with independently watermarked copies of the data.
2. It is robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, re-sampling, and re-quantization, including dithering and recompression and rotation, translation, cropping and scaling.

1.2.1.1.4 Least significant bits modification (LSB)

This approach is one of the simple approaches and makes use of least significant bits for embedding the watermarks. This technique stands well against cropping but is inefficient against noise addition and lossy compression and results in reseting LSB to 1. The approach is to generate the random generated to determine the LSB bits to modify and embed the watermark in the image. This technique can improve the security and prevent the third party from tracing the watermark, yet it is vulnerable against substitution of LSBs by a constant.

1.2.1.2 Frequency domain

In frequency domain, DCT, FFT and DWT methods are used for data transformation. Wavelet transform decompose an image into a set of band limited components that can be reassembled to reconstruct the original image without error. Linear programming optimized the Wavelet domain watermarking method. In Object based image watermarking technique, a watermark that embeds in distributed of an original data is very difficult to delete.

1.2.1.2.1 A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image

This approach first inserts the watermark into the middle-frequency range. Filter banks can be saved for the watermark embedding and the middle-frequency band to insert the watermark is chosen the coefficient in that band of the image is replace by the watermark.

The advantages of this approach:

1. This technique achieves both spatial and frequency localization.
2. It is both perceptual invisibility and robustness to compression.
3. It is robustness to noise, image processing techniques, median filter, geometric transform.

1.2.1.2.2 Hierarchical Watermarking Depending on Local Constraints

In this approach, the watermark is embedded according to two keys. The first key is used to embed a code bit in a block of pixels. The second bit is used to generate the whole sequence of code bits. The watermark is embedded in spatial domain by adding or subtracting a random digital pattern to the given image signal depends on the local energy distribution. The embedding depth level depends on the spectral density distribution of DCT coefficients and on the JPEG quantization table and inserts the watermark in the low frequency component. The depth label consists of a set of bits that are embedded locally in a rectangular set of blocks and it is repeated over the entire image. After detecting individual bits, the retrieve label is verified by performing a XOR operation to the watermark code.

1.2.1.2.3 Hybrid Watermarking

In this method, watermark can be embedded into both spatial and frequency domain.

1. A Hybrid Watermark for Tamper Detection in Digital Image – A hybrid image authentication watermark can be obtained as a combination of fragile and a robust watermark. The fragile watermark has the advantages that it has good localization and security properties. The hybrid watermark can be used to precisely identify changes as well as distinguish malicious tamper from simple operations. The authentication can be done without accessing any information about the original image.
2. Effective Hybrid Digital Watermarking Scheme Using Direct Sequence-Spread Spectrum Method – in this scheme, a watermark image is produced using the personal ID of copyrighter which is inserted into the original images and the watermark image is detected. It is an extension of the spread-spectrum watermarking scheme which combine key with logo method. Binary image is used as watermark image, and the degradation of image quality between original image and watermarked image is applied to confirm required invisibility in watermark system and watermark robustness is applied to protect a attack from the outside are analyzed using the values of PSNR of the watermark image.

1.2.2 Audio Watermarking

With the development of digital video and image watermarking, digital audio watermarking provides a special challenging issue because

1. Data hiding is not audible otherwise it will mask the original audio signal that can be easily tampered with and removed,
2. The human auditory system (HAS) operates over a wide dynamic range between 20 Hz to 20 kHz, therefore it is difficult to embed outside this rage,
3. There is a limited area of embedding the data.

Audio watermarking techniques [7] mainly focus on four characteristics, which are (1) low bit coding, (2) phase coding, (3) spread spectrum-based coding and (4) echo hiding.

1.2.2.1 Low-Bit Coding

In the low-bit coding technique, the watermark in an audio signal is embedded by replacing the least significant bit of each sampling point by a coded binary string corresponding to the watermark.

1.2.2.2 Phase Coding

Phase coding is one of the most efficient coding schemes in term of the signal-to-noise ratio because in this approach, it cannot be found any difference caused by a smooth phase shift, even though the signal patterns may change dramatically.

1.2.2.3 Spread Spectrum

The spread spectrum technique is intended to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible.

1.2.2.4 Echo Hiding

Echo hiding is a method for embedding information into an audio signal in such a way that the original signal is not degraded perceivably. This approach embeds data by introducing an echo. The value of a hidden datum corresponds to the time delay of the echo and its amplitude. The echo delays are selected to be less than the detectable hearing limited.

1.2.2.5 Affine Resistant Digital Audio Watermarking Using Template Matching

This approach is used for embedding a digital watermark inaudibly into an audio clip according to the difference between two half blocks of each block. This scheme does not require any host-related information for watermark extraction. The embedded watermark is robust to common audio signal manipulations, such as MP3 compression, time shifting, cropping, time scaling, D/A A/D conversion, insertion, deletion, re-sampling, re-quantization and filtering. Two kinds of information are hidden in the audio: the owner's information and a synchronization template. The owner's information is a binary image provided by the copyright owner, which can be words, numbers, a signature, a personal seal or an organization's logo. The synchronization template is generated by a random number generator controlled by a secret key and is used for synchronizing the signal caused by time shifting, cropping and time scaling attacks. These information are combined together and isolated by another secret key before embedding. This technique can be applied to automatically search for a protected audio from an audio database by first matching the synchronization template and then show the owner's information if it is claimed to have been watermarked.

1.2.2.6 Digital Audio Watermarking Based-on Multiple-Bit Hopping and Human Auditory System:

To optimally balance the audibility and robustness when embedding and extracting watermarks, the embedding scheme is high related to audio content by making use of the properties of human auditory system and multiple-bit hopping technique. The watermark embedding design is based on audio content and HAS. With content-adaptive embedding scheme, the embedding parameter for setting up the embedding process will vary with the content of the audio signal. Therefore, this technique involves segmenting an audio signal into frames in time domain, classifying the frames as belongs to one of several known classes and then encoding each frame

with an appropriate embedding scheme. To enhance the robustness and resistance of the embedded watermark, a multiple-bit hopping technique is employed. In this method, instead of embedding one bit into an audio frame, multiple bits with different time delay can be embedded into each audio sub-frame.

1.2.2.7 Muteness-Based Audio Watermarking Technique:

In this audio watermarking approach, the audio counterparts of text spaces are periods of silence. In audio signal, a mute period offers the following advantages [33]:

1. A mute period is an integral part of any audio signal which cannot be omitted since it represents an integral part of the studio signal.
2. It occurs randomly in audio signal which is generated by the music process.
3. A mute period represents a real time interval that will not be decreased when compressed.

In this approach, the audio watermarking technique is a muteness-based which offers the following features:

a) It extends the mute periods in an audio signal without any perceptual difference to the average human auditory system.

b) The extension of mute periods carries the same amplitude such that it will blend with the original and will not attract any attention.

c) It does not require the original signal to extract the watermark.

1.2.3. Video Watermarking Techniques

Cox et al. [1] described an approach for a watermark to be efficient to attack; it must be placed in perceptually significant areas of the image. The watermark was based on random samples of a N(0,1) distribution. These samples were added to a

large number of DCT coefficients [1] of the original image, and the inverse DCT was taken to retrieve the watermarked image. In the detection process, the watermark is extracted from the DCT of a suspected image. The Extraction can be done based on the knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient is computed and set to a threshold which is used to detect the watermark. This approach is robust to image scaling, JPEG coding, dithering, cropping, and rescanning [34].

Xia, Boncelet, and Arce [2] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). In this method, the watermark formed as Gaussian noise is added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. A part of the watermark is extracted and correlated with that part of the original watermark. If the cross-correlation was above a threshold, then the watermark is detected, otherwise the image is decomposed into finer and finer bands until the entire extracted watermark is correlated with the entire original watermark. This approach is very useful when embedded zero-tree wavelet compression and halftoning is performed on the watermarked images.

Bartolini et al. [3] generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark.

Kundur and Hatzinakos [4] proposed an approach in which the watermark is embedded in the wavelet domain. The strength of the watermark is determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations.

Delaigle et al. [5] proposed another watermarking scheme based on the Human Visual System. Binary m-sequences is generated and then modulated on a random carrier. This image is considered as the watermark and it is masked based

upon the contrast between the original signal and the modulated image. The masked watermark is added to the original image to form the watermarked image. This technique is applicable to additive noise, JPEG coding, and rescanning.

Craver et al [6] modified the Cox et al. algorithm that certain watermarking techniques are susceptible to counterfeit attacks. As the approach proposed by Cox et al. can be attacked by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark. To prevent this situation, the Cox et al. algorithm modifies by making the watermark dependent on the original image. This approach is less susceptible to counterfeiting and maintained robustness.

Bas, Chassery, and Davoine [7] introduced another watermarking system using fractal codes. A map is composed from 8x8 blocks of the original image and from the image's DCT. The watermark is added to the map to produce a marked image. Fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique is robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

II. Swarm Intelligence

Swarm intelligence (SI) is a branch of artificial intelligence (AI) discipline which mainly concerns with the design of intelligent multi-agent systems by taking inspiration from the collective behavior of social insects such as ants, termites, bees, and wasps, as well as from other animal societies such as flocks of birds or schools of fish. The concept of swarm was first introduced by Georado Beni and Xing in 1989.

Swarm intelligence works on two principles: Self Organization and Stigmergy.

In 1999, Bonabeau defined self organization "as a set of dynamical mechanisms whereby structures appear at the global level of a system from interactions of its

lower-level components" [26]. Stigmergy is associated with two words stigma and ergon (stigma (sting) + ergon (work) = "stimulation by work"). Stigmergy is based on the principle that, an environment serves as a work state memory where work does not depend on specific agents. Therefore, the coordination of tasks and the regulation of constructions do not depend directly on the workers, but on the constructions themselves. As there is no centralized control structure dictating how individual agents should behave, the agents work randomly and interactions between such agents lead to the emergence of "intelligent" global behavior, unknown to the individual agents. Some of the notable swarm based techniques such as Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Artificial Bee Colony Optimization (ABCO) are discussed here.

1. Ant Colony Optimization

Marco Dorigo introduced the first ACO algorithms in early1990s [27][28]. The development of these algorithms was inspired by the observation of ant colonies. Ants initially move randomly in order to locate a food source. As soon as they find a food source, it evaluates the quantity and the quality of the food and carry the food to their nest and deposit pheromone traces along the trail. Subsequently, ants decide on which of the available paths they shall follow based on the pheromone concentration deposited on each particular path. Paths with greater pheromone concentration have higher probability of being selected. Ants that follow the shortest path return to their nests earlier and pheromone on that path is reinforced with an additional amount sooner than the one in the longer path. The pheromone trails will guide other ants to the food source. Therefore, the selection among the paths is biased toward the shortest path.

A model has been designed for the study of the ants behavior. Ants begin from a source node of a graph *G(N,A)* and try to reach a destination node following the shortest path. To each arc *(i,j)* of a graph an amount of artificial pheromone is deposited $\tau_{i,j}$. This information can be read and written by the ants to govern their movement to the next node. Specifically, the probability of an ant *k* located at a node *i* of choosing next node *j* to be visited is calculated as

$$p_{ij}^{k} = \begin{cases} \dfrac{\tau_{ij}^{a}}{\sum_{l \in N_i^k} \tau_{il}^{a}} if j \in N_i^k \\ 0 if j \notin N_i^k \end{cases} \qquad (1.1)$$

Where N_i^k of the ant *k* when in node *i* contains in node directly connected to *i*, except the predecessor of *i*. α is a parameter for controlling convergence speed. When the ant reaches its destination it has to return to the source. In backward mode the ants deposit pheromone along the trail. Normally, the ant will attempt to follow the same route but if that route contains loops then it must eliminate them first, in order to avoid the problem of self-reinforcing loops. The new amount of pheromone in the arc *(i,j)* after ant k has traversed it in backward mode is calculated as:

$$\tau_{ij} \leftarrow \tau_{ij} + \Delta\tau^{k} \qquad (1.2)$$

Pheromone trails evaporate over time. This mechanism can be seen as a way to avoid the problem of convergence to sub optimal paths. Pheromone evaporation is simulated by applying the following equation to all arcs:

$$\tau_{ij} \leftarrow (1-p)\tau_{ij}, \forall (i,j) \in A \qquad (1.3)$$

Where *p (0,1]* is a constant.

2. Artificial Bee Colony Optimization

Artificial Bee Colony (ABC) algorithm is introduced by Dervis Karaboga in 2005 [29], motivated by the intelligent behavior of honey bees for optimizing numerical problems. The algorithm is specifically based on the model proposed by Tereshko and Loengarov (2005) for the foraging behavior of honey bee colonies [30]. The main objective of this model is to find out how the synergistic information exchanging interactions between the individuals leads to globally intelligent. The model has following:

a. Food Sources: The value of a food source to a bee depends on many factors including its proximity to the nest, richness or concentration of energy and the ease of extracting this energy.

b. Employed Foragers: Employed foragers are associated with a particular food source which they are currently exploiting or are "employed" at. They carry with them information about this particular source, its distance and direction from the nest and the profitability of the source. Employed foragers will share this information with a certain probability. The greater the profitability of the food source, the higher the probability the honeybee will do a waggle dance and share her information with her nest mates. Employed foragers are only locally informed – they know only of the food source they are currently exploiting and continue frequenting this food source until it is depleted, at which point they become unemployed foragers.

c. Unemployed Foragers: Unemployed foragers are looking for a food source to exploit. There are two types of unemployed foragers,

    i) Scouts, who search the environment surrounding the nest in search of new food sources

    ii) Onlookers, who are waiting in the nest find a food source through the information shared by employed foragers

At the initial stage, a set of food source positions are randomly selected by the bees and their nectar amounts are determined. Then these bees come into the hive and share the nectar information of the sources with the bees waiting on the dance area within the hive. After sharing the information, every employed bee goes to the food source area visited by her at the previous cycle since that food source exists in her memory and then chooses a new food source by means of visual information in the neighborhood of the present one. An onlooker bee prefers a food source area depending on the nectar information distributed by the employed bees on the dance area. As the nectar amount of a food source increases, the probability with which that food source is chosen by an onlooker increases. Hence, the dance of employed bees carrying higher nectar recruits the onlookers for the food source areas with higher

nectar amount. After arriving at the selected area, she chooses a new food source in the neighborhood of the one in the memory depending on visual information. Visual information is based on the comparison of food source positions. When the nectar of a food source is abandoned by the bees, a new food source is randomly determined by a scout bee and replaced with the abandoned one. In the model, at each cycle at most one scout goes outside for searching a new food source and the number of employed and onlooker bees were equal.

3. Particle Swarm Optimization

Particle Swarm Optimization (PSO) [15] [13] was invented by Kennedy and Eberhart while attempting to simulate the graceful motion of swarms of birds as part of a socio cognitive study investigating the notion of "collective intelligence" in biological populations. The algorithm begins with the initialization of random solutions. Each solution is initialized a randomized velocity and potential solutions called particles that searches the space. Each particle keeps track of its position achieved so far called pbest value. Another best value is tracked by global which is the best value and its location obtained so far by any particle in the population called gbest value. First, the positions, x^i_k , and velocities, v^i_k , of the initial swarm of particles are randomly generated using upper and lower bounds on the design variables values, x_{min} and x_{max} , as expressed in Equations 3.1 and 3.2. The positions and velocities are given in a vector format with the superscript and subscript denoting the i^{th} particle at time *k*. [17] In Equations 1 and 2, rand is a uniformly distributed random variable that can take any value between 0 and 1. This initialization process allows the swarm particles to be randomly distributed across the design space.

$$x_0^i = x_{\min} + rand\left(x_{\max} - x_{\min}\right) \tag{1.4}$$

$$v_0^i = \frac{x_{\min} + rand\left(x_{\max} - x_{\min}\right)}{\Delta t} \tag{1.5}$$

The next step is to update the velocities of all particles at time *k+1* using the particles objective or fitness values which are functions of the particles current positions *k*. The fitness function value of a particle determines which particle has the best global value in the current swarm, p^g_k , and also determines the best position of each particle over time, p^i , i.e. in current and all previous moves. The velocity update formula uses these two pieces of information for each particle in the swarm along with the effect of current motion, v^i_k , to provide a search direction, v^i_{k+1}, for the next iteration. The velocity update formula includes some random parameters, represented by the uniformly distributed variables, *rand*, to ensure good coverage of the design space and avoid entrapment in local optima. The three values that effect the new search direction, namely, current motion, particle own memory, and swarm influence, are incorporated via a summation approach as shown in Equation 3.3 with three weight factors, namely, inertia factor, *w*, self confidence factor, c_1 , and swarm confidence factor, c_2 , respectively.

$$v^i_{k+1} = wv^i_k + c_1 rand\left(\frac{p^i - x^i_k}{\Delta t}\right) + c_1 rand\left(\frac{p^g_k - x^i_k}{\Delta t}\right) \quad (1.6)$$

The position update is the last step in each iteration. The position of each particle is updated using its velocity vector as shown in Equation 4.4.

$$x^i_{k+1} = x^i{}_k + v^i_{k+1}\Delta t \quad (1.7)$$

4. Genetic Algorithm

Genetic Algorithm (GA) belongs to the family of evolutionary algorithms inspired by evolution natural behavior like selection, crossover, mutation at the level of cells. Genetic Algorithm was developed by Goldberg aiming to find the best solution in solving optimization problems. This algorithm works by creating set (population) of candidate solutions which are also called individuals, at the initial stage. Every candidate solution has its own set of properties (chromosomes) and these properties alterable and mutated. Generally binary strings i.e., 0s and 1s are used to represent these solutions. The evolution starts from a set of individuals that are randomly generated. This process is iterative and each iteration is called a generation. Every

individual has a fitness which is the objective function's value at each generation and this fitness is to be evaluated. Based on the fitness, individuals are selected from the current set and a new generation is formed by modifying (mutated) the individuals properties. In the next iteration the new generated individual is used. The algorithm is terminated after it reaches the highest number of generations or after reaching a fitness satisfaction level.

The strength of GA lies in its parallel searching nature. The genetic operators are sometimes weak even though solutions may continue to be part of the makeup of future candidate solutions. The genetic operators used are central to the success of the search. All GAs requires some form of recombination, as this allows the creation of new solutions, a higher probability of exhibiting a good performance. Crossover is the principal genetic operator, whereas mutation is used much less frequently. Crossover attempts to preserve the beneficial aspects of candidate solutions and to eliminate undesirable components, while the random nature of mutation is probably more likely to degrade a strong candidate solution than to improve it. By restricting the reproduction of weak candidates, GAs eliminates not only that solution but also all of its descendants. This tends to make the algorithm likely to converge towards optimal solutions within a few generations.

As compared with GA, PSO [32] also begins with a group of a randomly generated population and utilizes fitness value to evaluate the population. They all update the population and search for the optimum with random techniques. A large inertia weight facilitates global exploration (search in new areas), while a small one tends to assist local exploration. The main difference between the PSO approach and GA is that PSO does not have genetic operators such as crossover and mutation. Particles update themselves with the internal velocity; they also have a memory that is important to the algorithm. In GA, chromosomes share information with each other, thus the whole population moves like one group towards an optimal area. In PSO, only the 'best' particle gives out the information to others. It is a one-way information sharing mechanism, the evolution only looks for the best solution. All the particles

tend to converge to the best solution quickly. As compared to GAs, the advantages of PSO are that PSO is easy to implement and there are few parameters to adjust.

1.3 ORGANIZATION OF THESIS

The remainder of this paper is organized as the following. Chapter II details the proposed methodology. In Chapter III shows experimental results and evaluates the performance of the proposed system and finally, concludes the thesis and states some possible future work directions.

CHAPTER 2

PROPOSED WORK

Most of the existing algorithms provide better solution for embedding the watermark into the digital video without declining the quality of the video file. But some of the techniques has bad channel interference therefore, the watermarks gets destroyed by adding random bits labeled. Our proposed method tries to address the problem embedding the watermarks in video better security and as the motion vector hiding the watermark information can be more effective to use the information of video bit stream. The proposed methodology also survives the attacks on the network. As the marking motion vectors are robust against transmission error on noisy and bandwidth channels [37].

In video image data, successive frames share same context. The inconsistent modification of similar regions such as the same object regions in successive frames cause the visual artifact when video sequence is presented.

a. METHODOLOGY

In this work we have made an approach of selecting the motion vector based on the optimization technique such as Particle Swarm Optimization and Rough sets. The image frames extracted from the video sequence are subjected to preprocessing. The watermark image is generated by the Discrete Wavelet Transform (DWT) [25] [36].

DWT enumerates the high and the low frequency components by splitting the image into its respective frequency components. The high frequency components dedicated for the edge detection whereas the low frequency components are again bifurcated into high and low frequency components. The purpose of watermarking is served by the high frequency components as the human eye is sensitive on the edge variations. So, for the high performance the blue channel is transformed into DWT and the watermark is embedded from HL3 sub-band of the blue channel of the host video frame. The algorithm searches each frame pixel values for selecting the motion vectors. This is done by updating the current pixel position and velocities as the particles in the search space. The objective function is evaluated for each pixel values to explore the entire image for feature selection and to obtain the optimal motion vectors [36]. The rough-set draws the boundary for image region with α and β values. Each region is optimized individually for find the features values and combined to get the optimal motion vectors.

Rough Set

Rough set theory is a new mathematical approach to imprecision, vagueness and uncertainty. In an information system, every object of the universe is associated with some information. Objects characterized by the same information are indiscernible with respect to the available information about them. Any set of objects is called an elementary set. The set containing the vagueness can be termed as rough set. A rough set is the approximation of a vague concept by a pair of precise concepts, called lower and upper approximations.

The fundamental concept behind Rough Set Theory [13] is the approximation of lower and upper spaces of a set, the approximation of spaces being the formal classification of knowledge regarding the interest domain. The subset generated by lower approximations is characterized by objects that will definitely form part of an interest subset, whereas the upper approximation is characterized by objects that will possibly form part of an interest subset. Every subset defined through upper and lower approximation is known as Rough Set.

There are two types of approximations that are used in Rough Sets Theory.

a. Lower Approximation (B_low)

Lower Approximation is a description of the domain objects that are known with certainty to belong to the subset of interest. The Lower Approximation Set of a set X, with regard to R is the set of all of objects, which certainly can be classified with X regarding R, that is, set B_low.

$$\text{B\_low} = \bigcup \{Y \in U / B : Y \subseteq X\}$$

b. Upper Approximation (B_up)

Upper Approximation is a description of the objects that possibly belong to the subset of interest. The Upper Approximation Set of a set X regarding R is the set of all of objects which can be possibly classified with X regarding R, that is, set B_up.

$$\text{B\_up} = \bigcup \{Y \in U / B : Y \cap X \neq \phi\}$$

c. Boundary Region (BR)

Boundary Region is description of the objects that of a set X regarding R is the set of all the objects, which cannot be classified neither as X nor -X regarding R.

If the boundary region is a set X =∅ (Empty), then the set is considered "Crisp", that is, exact in relation to R; otherwise, if the boundary region is a set X ≠ ∅ (empty) the set X "Rough" is considered. In that the boundary region is *BR = B_up – B_low*.

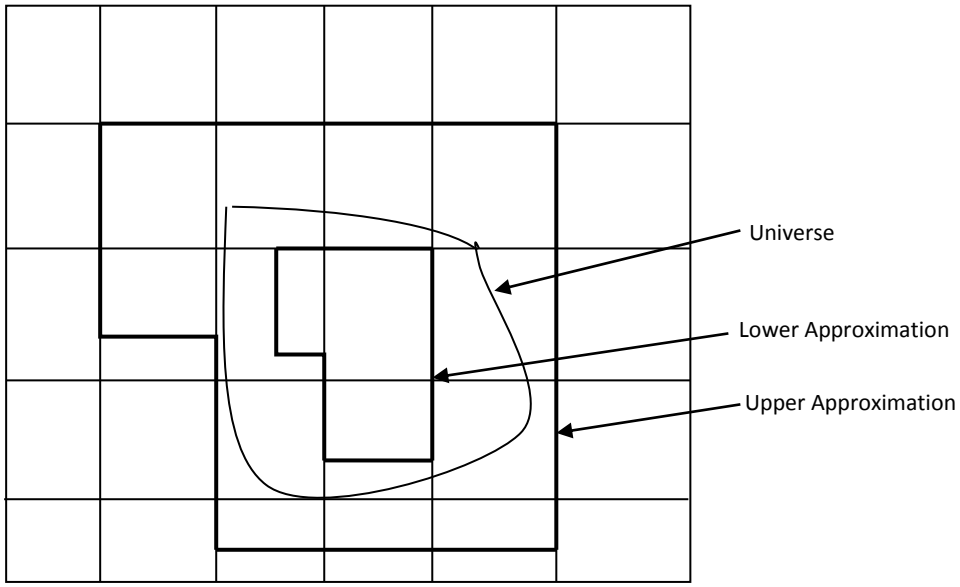

Fig 3. The Rough boundaries

The rough set theory has the following characteristics:

1. Each set is considered as an interval or rough set i.e. each interval/rough set is grouped, where lower and upper approximations B_low and B_up are characteristics of rough set X.

2. According to the elementary set theory, the data point should belong to atleast one set.

   a) An object *v* can be part of at most one lower approximation. This implies that any two lower approximations do not overlap.

   b) An object *v* that is member of a lower approximation of a set is also part of its upper approximation *(v∈B_low → v∈B_up)*. This implies that a lower

approximation of a set is a subset of its corresponding upper approximation *(B_low ⊆ B_up)*.

c) If an object *v* is not part of any lower approximation, it belongs to two or more upper approximations. This implies that an object cannot belong to only a single boundary region but not in upper approximation.

ii. Steps of algorithm

The entire proposed methodology is divided into different phase as detailed below:

A. Video Input

The video image is taken as the input to the algorithm.

B. Framing of video

A color image extracted from the video file at instance of time is known as a frame. These frames are preprocessed.

C. Watermark Generation

The DWT is performed for the image watermark. The image is decomposed into the components of partitioned frame into four sub-bands such as HH, HL, LH and LL with the aid of the DWT to attain the transformed frames. The low frequency sub-bands (HL, LH) are selected for transformation. A similarity matrix of the permuted image to embed is chosen from sub-bands. The upper part of the similarity matrix is embedded into the HL sub-band and the lower part of the similarity matrix into the LH sub-band. The HL and LH sub-bands used to embed the permuted watermark image are divided into four parts as per the similarity matrix. The lower part embedding part of the similarity matrix of the HL and LH

bands is chosen for embedding the two similar parts of the watermark image. The mean value and the maximum value mean (Up), max (Ep) of the chosen embedding part pE . The image is embedded into the cover image on each band value. Mathematically, The discrete wavelet transform of an image *f(x,y)* of size *M xN* is defined by:

$$W_{\phi}(j_0,m,n)=\sqrt[1]{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\phi_{j_9,m,n}(x,y) \qquad (2.1)$$

$$W^{i}{}_{\psi}(j,m,n)=\sqrt[1]{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\psi^{i}{}_{j,m,n}(x,y) \qquad (2.2)$$

Where *i={H,V,D}* and j_0 is an arbitrary scale. $W_{\phi}(j_0,m,n)$ defines low frequency coefficients of *f(x,y)* at scale j_0 and $W^{i}{}_{\psi}(j,m,n)$ define the horizontal, vertical and diagonal details.

D. Apply PSO for motion vector selection

The initial parameters for the optimization such as population, number of thresholds, number of iterations, individual weight of particles, social weight of particles, inertial factor. For each round the search is done by each particle as image pixel values and updating the position and the velocity of each particle. The search terminates when exact features are obtained. The alpha and beta value of the boundary for the region determination is computed by the rough set where each approximation is decided on the basis of the non-overlapping regions such as lower and upper approximations.

Algorithm

The Algorithm

Input: The video file

Output: The optimal set of features

Step 1: Extract the spatial frames from video file

Step 2: Convert each frame into image file

Step 3: Generate the image watermark with DWT

Step 4: Set the parameter values population size, number of thresholds, number of iterations, individual weight of particles, social weight of particles, inertial factor

Repeat

For each image frame f_i

Step 5: if $Y(x_i) > Y(p_i)$ then $p_i \leftarrow x_i$

Step 6: Calculate the initial velocity of the particles

Step 7: Calculates the fitness value of each particles $Y(p_i)$

Step 8: Apply rough set theory for selecting boundaries

Step 9: Calculates the velocity of each particles for the grayscale or RGB image

Step 10: Update the particle position

Step 11: Obtain the best fitness value for each channel (grayscale or RGB)

Step 12: Obtain the feature set after PSO optimization.

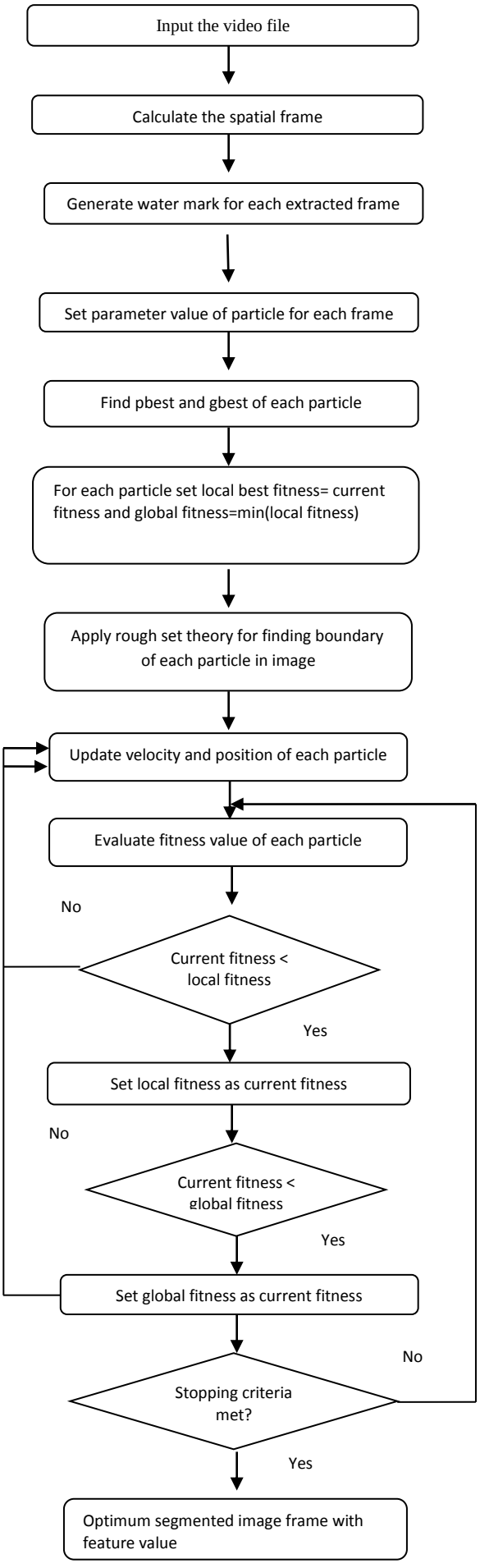

Fig 4. Flowchart of proposed method

a. WATERMARKING ATTACKS

It is important take into account that the watermarking system could be influenced by various kinds of attacks when it is applied in the copyright protection, content the authentication and so on. The watermark abilities against the attack in different application areas have different requirements and the ability against the attack is the most important performance of the Digital watermarking evaluation system.

The attack of video watermark is a video process which could weaken the watermark detection or cause polysemy to the watermark message. Deguillaume and Hartung [18,19] divide attacks of video watermark into simple attack, desynchronized attack, confused attack and removing watermark attack. The purpose of attacks is to make the corresponding testing tools of the video watermark system in such a way that it cannot recover watermarking signal or detect watermarking signal existence [23][24].

The following are some common attacks of video watermark:

i. Simple attack – it refers to unintentional attack which makes influence on the watermark information such as the loss of watermark information when coding video with all kinds of compression coding standards; the changes of the frame rate and spatial resolution when NTSC PAL and SECAM convert with video standard format; the change of the screen display formats such as 4/3, 16/9 and 2.11/1; the video editing processing of frame deletion, frame insertion and frame reintegration, the geometric distortion of video brought by digital-to-analogue conversion and analogue-to-digital conversion, all of this will make the video watermark be destructed.

ii. Desynchronized attack - it is necessary to know the location of embedded watermark for most of the watermarking

technologies. Desynchronized attack is to destroy the synchronicities of the video sequences and watermark on space or time, in order to make the detection algorithm cannot detect watermarking information. The desynchronized attack generally adopts geometry transform, such as zoom, the translation of space direction, the translation of time direction, rotation, shear, pixel displacement, second sampling, insertion or extraction of pixels or cluster of pixels, etc.

iii. Confused attack – this type of attack produces confusion by means of mendacious watermark information or original video sequence which is put forward by Craver [14] in IBM and known as IBM attack. The principle is that the attackers defines faked watermark as reference model which is randomly generated and then subtract the reference model from the works with watermark and finally a faked work is generated. One or more additional watermark are embed into the image having in order to confuse the first watermark containing copyright information, then the copyright becomes uniqueness. In this way, the attacker could state copyright of the original works and the copyright protection function of digital watermark is challenged.

iv. Removing watermark attack - for analyzing the watermark data and estimating the watermark information in video image, the removing watermark attack separates the video image with the watermark information and abandons watermarking information, then gets video image without containing watermark information and it finally achieves the purpose of illegal theft. The common removing attack methods are collusion attacks, de-noising, determinate

nonlinear filtering, compression with image comprehensive model, and so on.

v. Wiener Attack

Wiener attack is a attack on the Rivest & Shannon Algorithm (RSA) [23]. This attack occurs when the implementation of the RSA algorithm goes wrong.

Suppose Alice and Bob have public keys (N,e) and (N',e') but $gcd(N,N') = p$ is prime. Then Eve can easily factor both Alice's and Bob's public moduli. One should choose the prime factors p and q of an RSA key in a suitably random way such as $p-1$ being a product of small primes, making $N = pq$ vulnerable to factorization via Pollard'sp−1 algorithm). Accidental collisions could still feasibly occur, but it is desirable to keep such collisions at a minimum.

Bob wants to invite Alice, Adam, and Adele to his birthday party, but doesn't want that shady Eve to crash it. Alice, Adam, and Adele have RSA keys $(N_1,3)$, $(N_2,3)$, and $(N_3,3)$, and because they know about the attack they have ensured that $gcd(N_1,N_2) = gcd(N_2,N_3) = gcd(N_3,N_1) = 1$. Bob's invitation is short enough so that, as an integer, m satisfies $0 < m < N_1,N_2,N_3$.

Bob sends $m^3 \bmod N_1$, $m^3 \bmod N_2$, and $m^3 \bmod N_3$ to Alice, Adam, and Adele, respectively. Eve intercepts the encrypted messages, and using the CRT, she can compute $m^3 N_1,N_2,N_3$ and mod $m^3 < N_1,N_2,N_3$. Eve recovers $m^3 \in Z$, the cube of the integer m. Taking the cube root of m3 (as a real number), Eve recovers m. Eve can take nth roots of real numbers with relative ease.

In general, if Bob sends the same message to n people and they all have the same public exponent ≤ n, then Eve can decrypt the message quickly. If $N = pq$ is a RSA modulus (with $p \approx q \approx \sqrt{N}$), then $N \approx \varphi(N)$. If $ed \equiv 1 \bmod m$ for some modulus m

≥ 1 and positive integers e and d, then d appears as a denominator in the convergents of e/m.

Wiener's idea is: [24] Since $ed \equiv 1 \bmod \varphi(N)$, d appears as a denominator in the continued fraction expansion of e/φ (N). If $N \approx \varphi(N)$,then e/N and $e/\varphi(N)$ have some convergents in small denominator.

Therefore, to design a preferable video watermark in order to resist a variety of deliberate and in-deliberate attacks is an important key of video watermark technology.

CHAPTER 3

RESULTS, DISCUSSION AND CONCLUSION

3.1 EXPERIMENTAL ENVIRONMENT

The experiment is performed on a 2.93 Gigahertz Intel Core i3 processor computer with 3 GB memory, running on Windows 2007. The algorithm is implemented in MatLab programming language.

3.2 RESULTS

Fig 5. Watermark embedded image with PSO

Fig 6. Result of Proposed method

The proposed watermarking algorithm is tested for the various host and watermark images. Here some results are given. To evaluate the performance of the proposed method, calculate PSNR (Peak Signal to Noise Ratio) and NCC (Normalized Cross Correlation) values. PSNR is widely used to measure imperceptibility between the original image and watermarked image. PSNR is defined by the eqn. (3.1). The similarity between the original and extract watermark image use to represent how algorithm is robust against noise that is calculated by NCC value. NCC is defined by eqn. (3.2)

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \qquad (3.1)$$

Where,

$$\text{MSE} = \frac{1}{M\ X\ N}\sum_{m=1}^{M}\sum_{n=1}^{N}[\ \text{I}(\text{m},\text{n}) - \ \text{I}_{\text{w}}\ (\text{m},\text{n})]^2 \qquad (3.2)$$

	Parameter		
	PSNR	**RMSE**	**NCC**
Existing Approach (Without Noise)	3.8305	77.2869	0.9018
Proposed Approach (Without Noise)	5.2077	76.7080	0.9282
Existing Approach (Gaussian Noise)	4.0104	78.2822	0.8920
Proposed Approach (Gaussian Noise)	5.5602	76.1025	0.9144

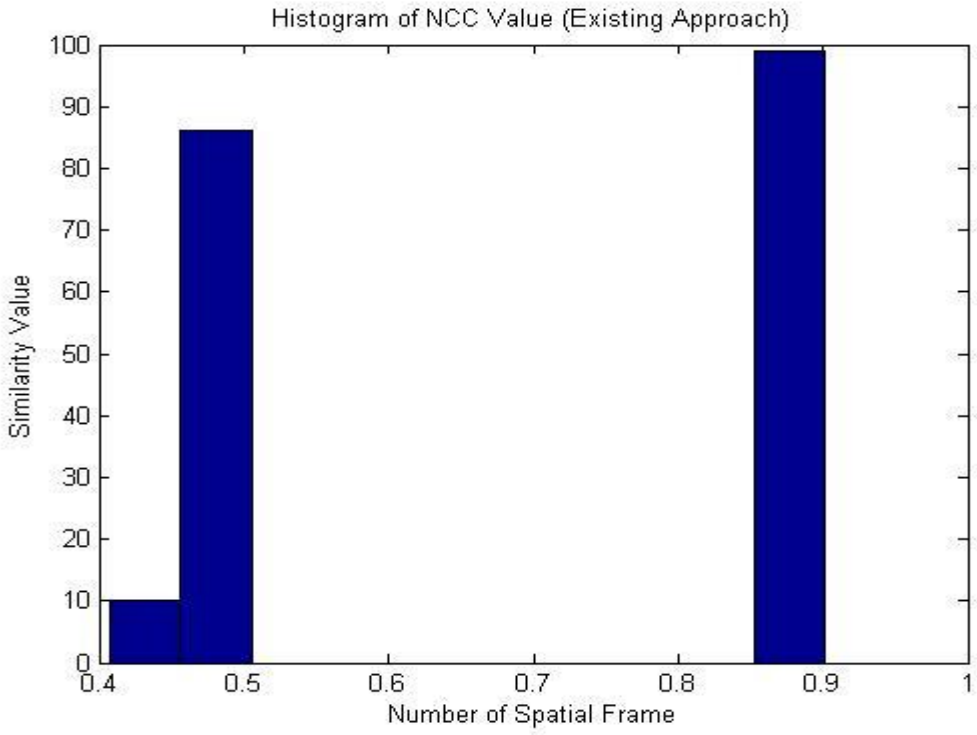

Fig 7. Histogram of NCC value

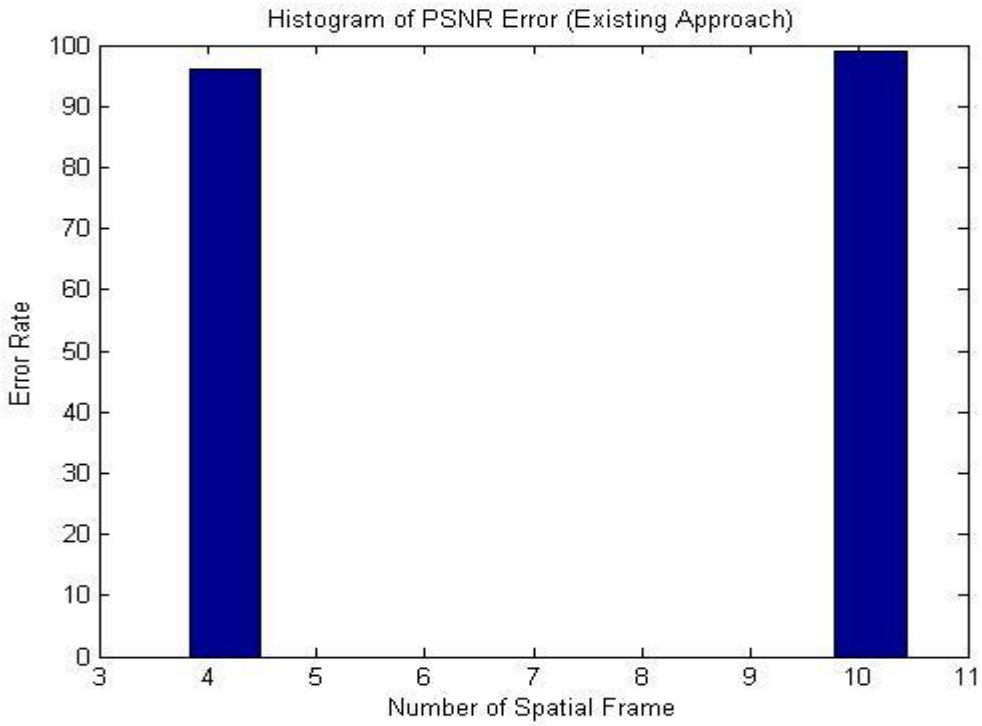

Fig 8. Histogram of PSNR Error

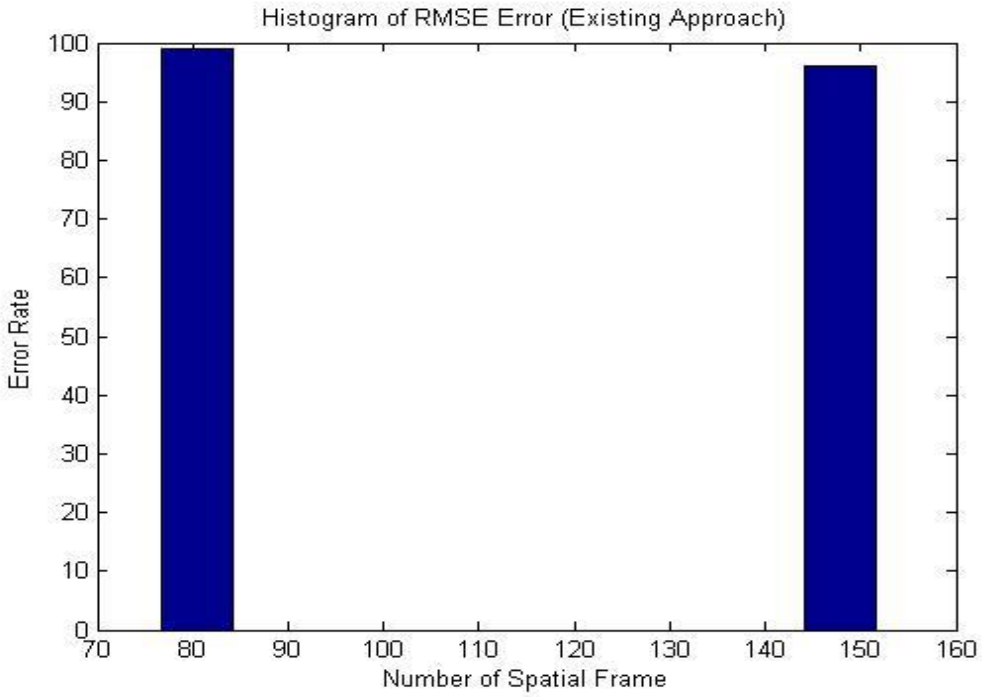

Fig 9. Histogram of RMSE Error

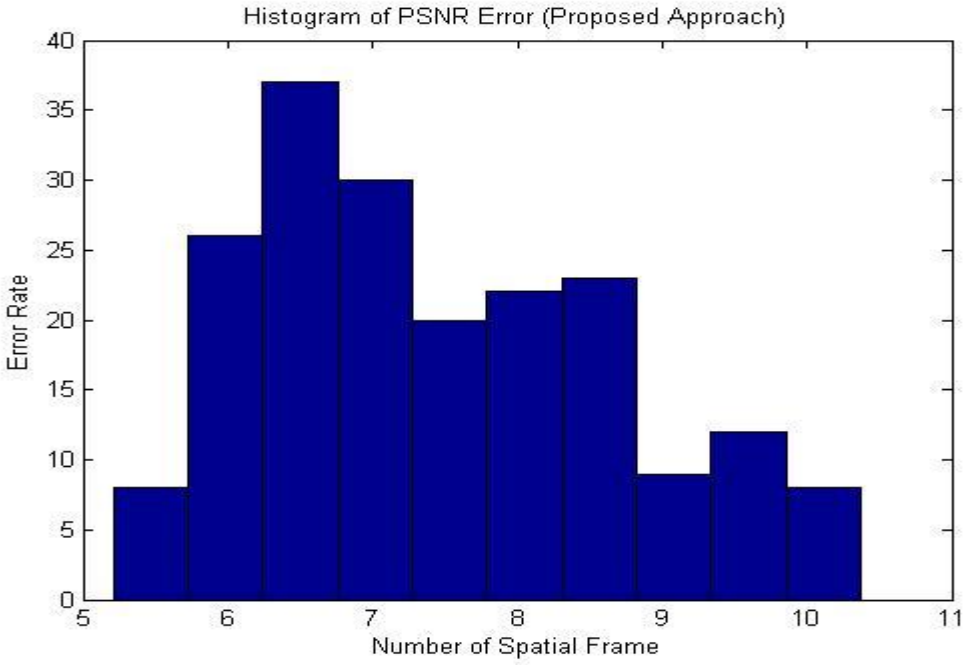

Fig10. Histogram of PSNR Error

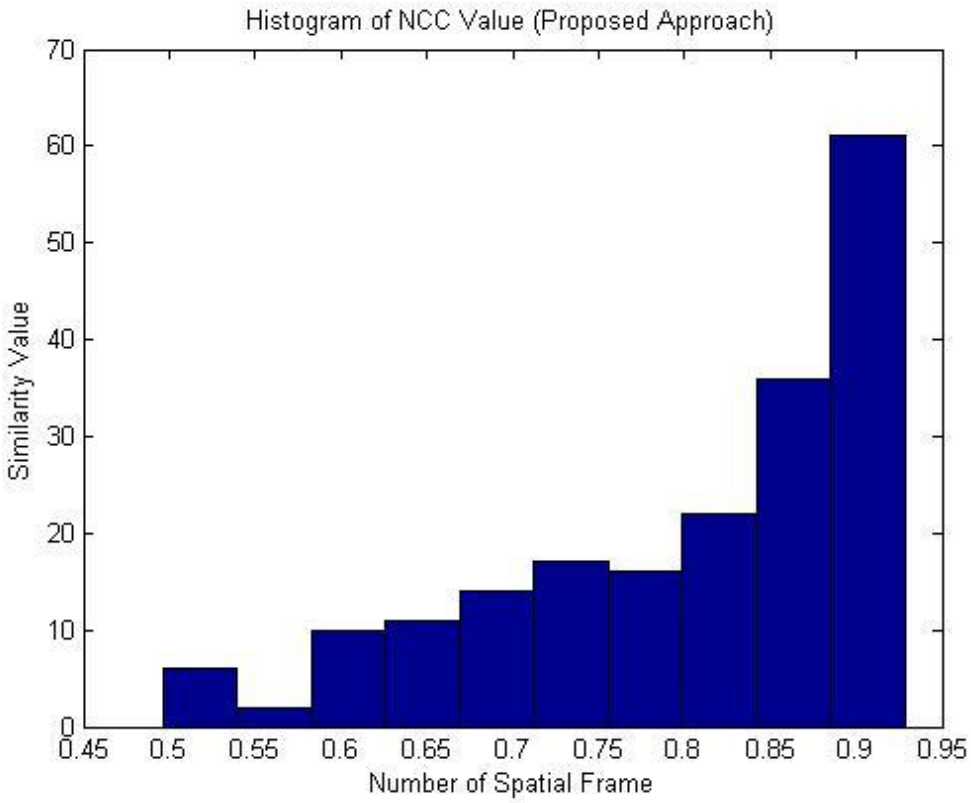

Fig11. Histogram of NCC value

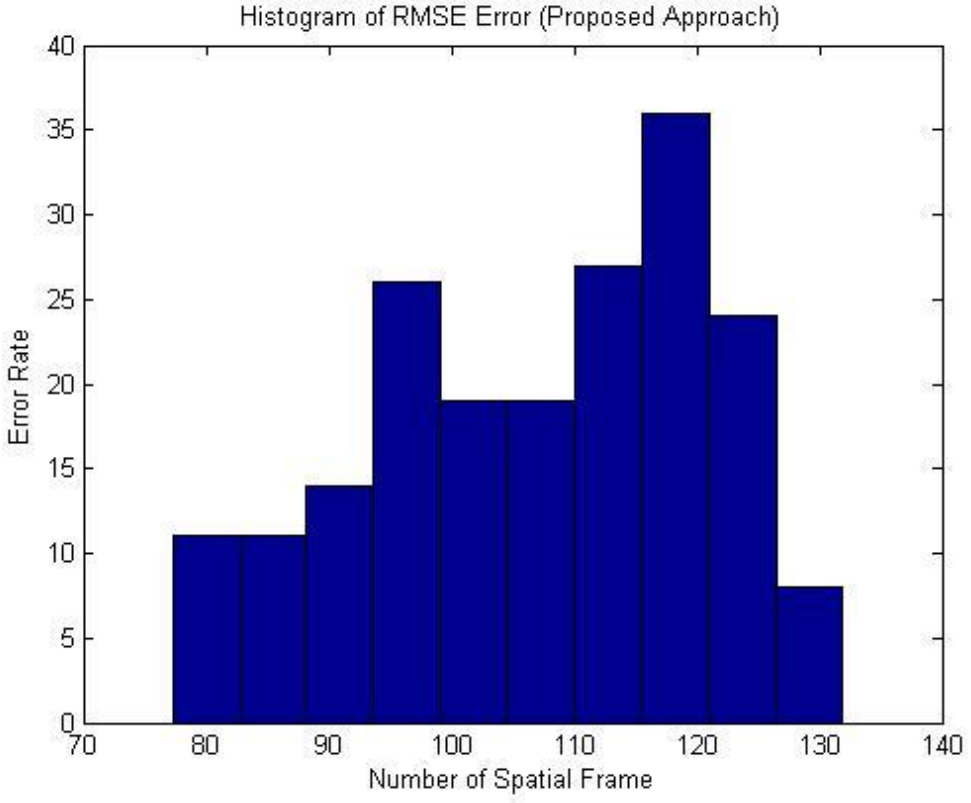

Fig 12. Histogram of RMSE Error

3.3 ANALYSIS

The performance of the proposed algorithm is evaluated using the Root Mean Square Error (RMSE) and Peak Signal to Noise Ratio (PSNR). In Fig 5, the pixel values of the all the frame image are embedded with the watermark. The regions is obtained from the rough set contains the most similar feature values. As a result, the application of PSO with initialization of each pixel in image frame, the entire search space is exploited for the feature vectors. With each iteration, the position and velocity is updated which updates the directional vectors of the feature.

Fig 6 shows the result of the proposed methodology highlighting the application of PSO with rough-set for selection of the optimum feature vectors. The histogram plot of RMSE error in fig 7 shows the similarity in the feature values after embedding the watermark and with the application of proposed approach. The histogram plot of PSNR error in fig 8 shows the performance evaluation of the proposed methodology. The plot shows the effect of the noise in each channel of watermarking. The ratio declines as the number of frames increases, the error is reduced. Hence the similarity of the optimum feature retains after embedding the watermark ensuring the originality of the data and security remains intact.

Table I demonstrating the PSNR value of each video frame. As it embeds the watermark in the identical frame of each video shots so here the PSNR value represent the average of total identical frames. The less the value of PSNR is the more perceptible the watermark is. It also shows the values of PSNR, RMSE and NCC without noise and Gaussian noise for the performance evaluation. The value with image without noise for the similarity measure of the NCC is 0.9282 and with the Gaussian noise is 0.9144 which indicates the robustness of algorithm for the watermarked image and the original image. Similarly the PSNR value of the algorithm is without noise 5.2077 and 5.5602 with the Gaussian noise. Hence we see that with introduction of the Gaussian noise the algorithm works well.

3.4 CONCLUSION

We propose a new optimal feature selection technique based on rough sets and Particle Swarm Optimization. It has the ability to quickly converge and a strong search capability in the problem space and can efficiently find minimal reducts. In the algorithm the inertia weight (w) and maximum velocity (Vmax) have an important impact on the performance of PSO. The selection of the parameters may be problem-dependent. The fitness function and position-updating strategy are also key factors in PSO for feature selection, which are enhanced with application of the rough set for the boundary values in the images. The experimental results show that the proposed work stands well as compared to the existing algorithms in the literature.

REFERENCES

[1] I. Cox and M. Miller, “Electronic watermarking: the first 50 years,” in IEEE Fourth Workshop on Multimedia Signal Processing, 2001, pp. 225 –230.

[2] N. Ahmed, T. Natarajan, and K. Rao, “Discrete cosine transform,” IEEE Transactions on Computers, vol. 100, no. 1, pp. 90–93, 1974.

[3] M. Shensa, “The discrete wavelet transform: Wedding the a trous and mallat algorithms,” IEEE Transactions on Signal Processing, vol. 40, no. 10, pp. 2464–2482, 1992.

[4] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, “Multimedia Data Embedding and Watermarking Technologies”, Proceedings of the IEEE, 86(6):10641087, June 1998

[5] G. Voyatzis, N. Nikolaides, I. Pitas, “Digital Watermarking: An Overview”, Proceedings of IX European Signal Processing Conference (EUSIPCO), pp. 13-16, Island of Rhodes, Greece, 8-11 September 1998.

[6] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[7] Xia, C. Boncelet, and G. Arce, “A Multiresolution Watermark for Digital Images,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[8] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, “Mask Building for Perceptually Hiding Frequency Embedded Watermarks,” Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.

[9] D. Kundur and D. Hatzinakos, “A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 544-547.

[10] J. Delaigle, C. De Vleeschouwer, and B. Macq, “Psychovisual Approach to Digital Picture Watermarking,” Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640, July 1998.

[11] S. Craver, N. Memon, B. Yeo, and M. Yeung, “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications,”

IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573-586, May 1998.

[12] P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.

[13] Hu, K., Lu, Y.C., Shi, C.Y., 2003. Feature ranking in rough sets. AI Communications 16(1), 41-50.

[14] Guyon, I., Elisseeff, A., 2003. An Introduction to Variable and Feature Selection. Journal of Machine Learning Research. 3, 1157-1182.

[15] Eberhart R.C., Shi, Y., 2001. Particle swarm optimization: Developments, applications and resources. Proc. IEEE Int. Conf. On Evolutionary Computation. Seoul, pp. 81-86.

[16] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," In Proc. Xiv Brazilian symp. Computer Graphics and Image Processing, pp. 179-182, Oct. 2001.

[17] Kutter M. Jordan F. and Ebrahimi T. Proposal of a Watermarking Technique for Hiding/Retrieving Datas in Compressed and Decompressed Video. In ISO/IEC/JTC1/SC29/WG11/MPEG97/M2281, 1997.

[18] Sun SH H, Lu ZH M and Niu X M. 2004 Digital watermarking technology and application Beijing: Science press

[19] Ma F Zh, Chen D. 2009 Differential Component Video Watermarking Algorithm Based on Motion Vector. Guang Dong: China Institute of Communications.134-138

[20] F.Hartung, J.K.Su, B.Girod. 1999 Spread spectrum watermarking: malicious attacks and counterattacks. Security and watermarking of Multimedia Contents, Proceeding of SPIE, 36(57):147-158

[21] F.Deguillaume, G.Csurka, T.Pun. 2000 Countermeasures for unintentional and intentional video watermarking attacks. Security and Watermarking of Multimedia Contents II, Proceeding of the SPIE, 39:346-357

[22] S.Craver, N.Memon, B.L.Yeo, M.M.Yeung. 1998 Resolving rightful ownerships with invisible watermarking techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, 16(4): 573-586

[23] J. Blomer, A. May, A Generalized Wiener Attack on RSA, University of Paderborn, Germany.

[24] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less thanN0.292, IEEE Trans. on Information Theory, Vol. 46(4), 2000

[25] P.Sharma and T. Jain, Robust Digital Watermarking for Coloured Images using SVD and DWT Technique, IEEE International Advance Computing Conference (IACC), pages 1024-1.27, 2014.

[26] D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm", Applied Soft Computing 8(2008), pp. 687-697, 2008.

[27] M. Dorigo, V. Maniezzo,and A.Colorni., Ant System: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics – Part B, 26(1):29–41, 1996.

[28] M.Dorigo and C.Blum., Ant colony optimization theory: A survey. Theoretical Computer Science, 344(2-3):243–278, 2005.

[29] Dervis Karaboga, "An Idea Based On Honey Bee Swarm For Numerical Optimization", Technical Report-TR06, October 2005.

[30] V. Tereshko, A. Loengarov, "Collective Decision-Making in Honey Bee Foraging Dynamics", Computing and Information Systems Journal, ISSN 1352-9404, vol. 9, No. 3, October 2005.

[31] K.T. Meetei, A Survey: Swarm Intelligence vs Genetic Algorithm, International Journal of Science and Research (IJSR), vol. 3, pages 231-235, 2014.

[32] K. O.Jones, Comparision of Genetic Algorithm and Particle Swarm Optimization, International Conference on Computer Systems and Technologies, 2005.

[33] R. T. Paul, Review of Robust Video Watermarking Techniques, International Journal of Computer Applications, no. 3, pages 90-95, 2011.

[34] A. Srivastava and D. Mistry, Digital Video Watermarking Techniques: A Review Study, International Journal of Scientific Research and Development, vol. 2, pages. 323-326, 2013.

[35] M. Kumar and A. Hensman, Robust digital video watermarking using reversible data hiding and visual cryptography, 24th IET Irish Signals and Systems Conference 2013, pages. 1-6, 2013.

[36] J. Panyavaraporn, Multiple video watermarking based on wavelet transform, 13th International Symposium on Communication and Information Technologies (ISCIT), pages. 397- 401, 2013.

[37] B. Goel and C. Agarwal, An optimized un-compressed video watermarking scheme based on SVD and DWT, 6th International Conference on Contemporary Computing (IC3), pages. 307-312, 2013.

[38] K. Raval and S. Jaffer, Digital watermarking with copyright authentication for image communication, International Conference on Intelligent Systems and Signal Processing (ISSP), pages. 111-116, 2013.