ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Image Authentication Using Advanced Watermarking and Multi Layered Coding

Bipin Dev S S[1], Kiran W S, ME, (PhD)[2],

PG Student, Department of ECE, Sivaji College of Engineering and Technology, Manivila, Kanyakumari Dist, Tamil Nadu, India[1]

Assistant Professor, Department of ECE, Sivaji College of Engineering and Technology, Manivila, Kanyakumari Dist, Tamil Nadu, India[2]

ABSTRACT: Public networks can be tracked and the datas may be extracted by intruder or hackers. To avoid this condition over the digital communication system, images are protected using the coding techniques and watermarking. The importance of this method is special kinds of watermarking scheme. It is known as encrypted-watermarking. Here, the source coding sections are dedicated mainly for compression. Channel coding is used to encrypt the compressed datas with the support of two sections of permutations and Reed-Solomon code used as the algorithm for coding process. Another important part is the hash generator for creating signature with respect to the input image. Least Significant Bits detector is used to identify the Least Significant Bits and Most Significant Bits. Most Significant Bits are utilized as the reference datas. Encrypted Watermarking block will generate the watermarking bits and it will be embedded with encrypted data bits to generate resultant watermarked image.

KEYWORDS: Reed-solomon code, Least Significant Bits, MostSignificantBits, SourceCoding, ChannelCoding, Watermarking

I. INTRODUCTION

In the digital communication systems authentication has an important role. Authentication over the data transfer,especially in the image transfering through a particular channel must be safer one. But now a days many kinds of noises, tampering issues, tracking problems are involved in the large scale. Due to this problems the normal image can be tampered and which can be converted in to ulter another one data or which may be loose. At the receiver end, It may get as in the format of noise. To overcome this, conditional multilayer of protection is essential for image transfer through a particular channel. In this proposed scheme multilayer of protection is provided for the image through image processing technique and data transfer scheme or methodology. Source coding and channel coding are itself acted as the protective layers for the corresponding data. Coding techniques are used to achieve compression as well as encryption for the image. Thus using these techniques maximum range of robustness and security can be achieved. In which advanced watermarking as well as hashing is used to provide self detection and avoidance of tracking of original data by the third party in a particular channel. Thus the maximizing of the protection level of the transfering image can be achieved more better than the old schemes. Mainly the watermarking is useful for tamper detection and recovering original image from received data. The importance of this method that the tolerable tampering rate must satisfy a certain threshold level. Beyond that the value must be vulnerable one and the original image reconstruction is not possible in that condition.Also certain parametric concept are utilizing to find out the levels of compression and transmission mode in the case of watermarking. Which can be varied at the transmitter end as the fragile type or block type of approaches are varying systematically. For this case supportive Wavelet Decomposition and DCT can be used. DWT is the another kinds of wavelet transform or decomposition technique used in many methods. Hash generators are also utilized with the watermarking scheme for improving the overall performance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

II. RELATED WORKS

Protection against localize image tampering as a simple method of hashing and create robust against image illegal manipulations in any kinds of format in the corresponding network for image transferring in the secure mode of operation [1].Image hashing is utilized for generating the look up table for the corresponding input image for more robustness and security image is processed in the multilayers. Comparison of the image and considered data streams for reference are used to preserve the image in the proper way. The benefit of the hash generation is the security providence[2]. Singular Value Decomposition and Non Negative matrix factorization are considered as the Dimension Reduction techniques. Which are used to maintain the essential features with the better performance over robust and secure image hashing [3]. Divided into blocks of the corresponding image is given as input to the processing sections. Fragile water marking scheme is used to provide protection for the image. In this method 2LSBs are used for watermarking. Set the hypo-LSB and LSB in the proper range [4].Image hashing function converts an image into a bit string or signature. Which can be used to provide security for the originality of the image. In this method an advanced image hashing scheme is provided that is secure and robust to abnormal changes for the original image[5]. Fragile watermarking scheme having the capability to perfectly recovering the original image from its tampered version[6].Local Binary pattern based histogram sequence method over biometric multimedia security systems are random numbers for robust and secure human authentication. Secret seed or hash key is used for generating pseudo random sequence and which is orthonormalized using Gram-Schmidt algorithm. Inner-product between the histogram vector and pseudo-random sequence is done. Biometric hashing is generated by using thresholding technique[10]. Enhancement of the robustness against rotation manipulations, the conventional Gabor filterization. Which are adapted as rotation invariant. The rotation-invariant filter is randomized to provide secure feature extraction. Mainly a novel dithered-LVQ based quantization scheme is proposed for robust hashing[16]. The simulation scheme is used for activating the system.In which the order of the data is changed. That means if a particular image is considered which can be subdivided into certain sub-layers as puzzles. The order of the sub-images are changed random manner and each of the layers are water marked separately[20].

III. METHODOLOGY

In the case of encrypted watermarking, Images are processed through certain steps. Which are acting as protective layers as well as codings. Each steps are explained below.

A. Proposed System

The Figure 2(a) is corresponded to the proposed system. Which is used to generate the watermarked image, it is also denoted as encrypted watermark image. It is the modified version of existing method. Important parts are sourcecoding, channel coding, LSB detection, permutation, hash generation and watermarking etc.

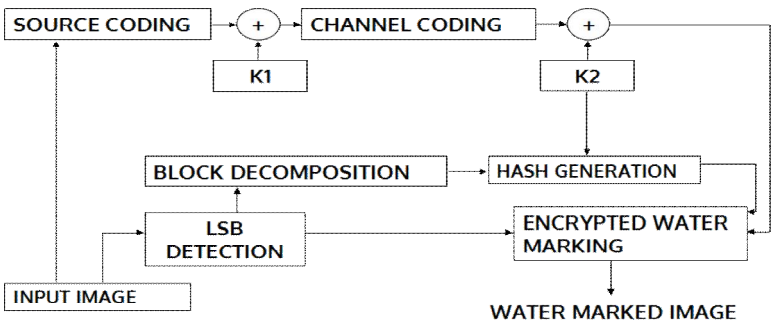

Figure 2(a) Proposed Block Diagram

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

At first, input image is applied to the source coding section and LSB detection section. In both of the parts different operations are carriedout. In the LSB detection least significant as well as most significant bits are generated. Which are used for hash generation and watermark production. Also provide reference bits in the embedding system. Source coding is compressing all images, which are given as input to the source coding section. Permutation is presented as two levels for adding secret keys to the processed and compressed data bits through coding operations. For this purpose and hashing secret keys are given through separate medium and keys are comparitively different one.
Channel coding is used to provide protection over the channel from noises and occurance of errors. For which block codes are generated in this section. Block decomposition is another kinds of compression technique and it is used in hash generation process. Hash generator is used to provide signature in the embedded section for generating watermark effectively. Embedding part is used to generate encrypted watermark of input image, which is the resultant output of this system.

B. Source Coding

At first the input image is applied to the source coding section. In which mainly the compression of the images carried out.Two sections are presented. Which are given as Wavelet Decomposition and encoding. In the case of wavelet decomposition, Discrete Wavelet Transform is carried out. Coding is utilized only for the compression and modulating the signals according the circumstances and conditions of the channels. Watermarking algorithms are mainly applied for the image protection over the communication channel. Which can be applied with the support of additional methods or using hash generators. Itself, Which having the ability to build up the protection over the image transfer from any distance without any kinds of error generating problems due to the channel faults or the faults creation by the trackers. Mainly the watermarking is useful for tamper detection and recovering original image from received data. The importance of this method that the tolerable tampering rate must satisfy a certain threshold level. Beyond that the value must be vulnerable one and the original image reconstruction is not possible in that condition. Also certain parametric concepts are utilizing to find out the levels of compression and transmission mode in the case of watermarking. Which can be varied at the transmitter end as the fragile type or block type of approaches are varying systematically. For this case supportive Wavelet Decomposition and DCT can be used. DWT is the another kinds of wavelet transform or decomposition technique used in many methods. Hash generators are also utilized with the watermarking scheme for improving the overall performance. Coding may be in the different strategies. According that, Which are classified in to different types. Coding techniques may be utilized as the simple encoding at the transmitter end as compression and decompression at the receiver end. In many techniques source coding as well as channel coding are utilizing but do not give the importance such as a security providence. In which any one of the method acts as the important supportive part for the watermarking stream without become as the security provider for the data stream itself. The important fact that if both the techniques can be used to provide extra security for each section of processing such as source coding as well as channel coding in the modern type of operations when compare with old methods. So, which is also having the data transfer influence in the wide range scale of control over data security as compression. Both of the wavelet decomposition and encoding are combinely known as SPIHT algorithm. Which is overall source coding carried out and generate compressed image.

C. Channel Coding

Channel Coding is the next section after the Source coding. The output from the source coding is the compressed data bits. Which are transferred to the channel coding for two divisions of permutations and taken as P1 and P2. P1 is carried out before channel coding and P2 is applied after it. RS code is supportive for the transmitting datas through a channel. Set of data bits are considered as block codes consists of total n number of bits. In this n bits, k bits are dedicated for datas and 2t bits are corresponded for parity bits or check bits. Check bits are used to control the operations over block codes.Thus the block codes are generated over the channel coding operations. Which are carried out with the support of a cyclic operations or the loops using permutations.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

D. LSB Detection

LSB Detection is used to find out the LSB bits or Least Significant Bits from the input image. Through this operation MSB bits are extracted. MSBs are Most Significant Bits utilizing as the reference bits and which is used as input to the hash generator. Reference bits are not processed and maintain it as in the normal format. Which are separately handled and store in the watermarking system without any change with other processed coded bits or LSBs of the size about 2bpp. With these reference data bits additionally certain MDHTR bits are included for supporting the overall performance of the system but which are becoming as the supportive part for reference section. It is a simplest block but which having very important role when compare its effectiveness.

Least significant bits and Most significant bits are used to eliminate whole data usage, It is unnecessary for next step processes.Through this process Most significant bits are generated in the other hand simultaneously with LSB bits. Which is used for two sections of operations. First one is transfered to the main blocks are given as source coding, channel coding etc. In these steps, corresponding data bits are compressed and encrypted. Encryption keys are essential under this step. After that the processed datas are lead to the embedding block. Another branch is turned to the block decomposition section. Here, data bits are reduced considerably. But which is not similar to the spiht algorithm methods. Simple form of compression with discrete cosine transform is carried out.

Maximum rate of compression is provided in this section. Rate is provided as the characteristics and properties of the processing image. Then the corresponding data bits are transfered to the hashing block or hashing bit generator in effective manner. Continuous steps are utilized for compression in this section of operation. Errors are removed as effective as possible, it is the important target. Which is achieved with these steps as decomposition and hashing function. Important role is mainly provided for decomposition for avoiding all kinds of errors and faults. Most significant bits are considered for this hashing operations and utilized for signature generation as well as reference bits generation. These two streams of datas are used for watermarking operation. Each of the datas the important decision making steps are involved for providing maximum compression and hash bits generations.

E. Hash Generation

Signature having the important role in the case of cryptography. Hash generators are the signature generating part. Which is using the algorithm as MD5. MD5 means Message Digest of version 5. Which is converting the data bits to the corresponding signature . Each of the image having its own signature with respect to the key. Here the key k2, Which is used in the permutation section k2 is utilized for generating hash bits. In the hash generation at first a simple step is carried out as block decomposition. This step the size of the datas are reduced considerably. Resultant blocks must be minimum in this step, When consider corresponding output. After that the decomposed data bits are transferred to the hash bits generating section. Hash is generating with the support of the key. Key can be generated by using security key generator section for the single usage or multistream usage. Key is utilized for generating the hash bits from the decomposed datas.

Decomposition may be achieved through matrix factorization or wavelet decomposition technique. Thus the ordering of the data stream can be changed with the support of the key. Which give the resultant value of hash bits. Which is the simplest form of authentication technique. But it is not sufficient in the new concepts or approaches. Thus the modifications also be applied for the hash generation. Signature must be in the proper format and randomized key generation and message digest type of streams or approaches are utilized for both the decomposition and signature creation.Which is the advanced form of technique used in the new kinds of hash generators. The Most Significant Bits (MSBs) are given to this hash generator followed by block decomposition. MSBs are about 6bpp, for reducing its size block decomposition is used. Then hash bits are generated using hash generators. Thus n_h is created with the size about 0.5bpp. This Hash bits are utilized for generating watermark. Hash bits are generated from the data bits of size 6bpp. Which is considered as input to block decomposition section of hash bit generator. Faulty measurements are eliminated with support of the decomposition and message digest streams. Thus the excess of unnecessary datas are removed in the corresponding data bits. Signature having 0.5bpp of size mentioned earlier. The enhanced datas are used for processing through the step decomposition operation. Hashbits are different for each of the input images. It is due to the data streams or secure data bits are generated with the help of input data bits, it is compressed earlier steps.The keys are generated randomly and combine with the compressed data sequences. Hash bits are transfered to the next subsections

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

are converting the signature to the watermark . Which is used for embedding operation in the watermarking block. Which is the resultant value used in the encrypted watermarking operation.

F. Embedding

In which watermarking algorithm is used to generate encrypted watermarking data bits. Watermarking algorithms are mainly applied for the image protection over the communication channel. Which can be applied with the support of additional methods or using hash generators. Itself, which having the ability to build up the protection over the image transfer from any distance without any kinds of error generating problems due to the channel faults or the faults creation by the trackers. Mainly the watermarking is useful for tamper detection and recovering original image from received data. Authentication over the data transfer, especially in the image transfering through a particular channel must be safer one. But now a days many kinds of noises, tampering issues, tracking problems are involved in the large scale. Due to this problems the normal image can be tampered and which can be converted in to another one data or which may be loose in the receiver end as get as in the format as noise. To overcome this, conditional multilayer of protection is essential for image transfer through a particular channel with improper characteristics mentioned earlier. In this proposed scheme multilayer of protection is provided for the image through image processing technique and data transfer scheme or methodology. Source coding and channel coding are itself acted as the protection guard for the corresponding data. Coding techniques are used to achieve compression as well as encryption for the image for utilization of maximum range of robustness and security. In which advanced watermarking as well as hashing is used to provide self detection and avoidance of tracking of original data by the third party in the corresponding channel. The importance of this method that the tolerable tampering rate must satisfy a certain threshold level. significant regions of cover Work in order for it to be robust to lossy compression, yet changes in these same regions are mostly affecting fidelity. As noted previously, early watermarking systems applied a global power constraint to satisfy fidelity constraints. It was recognized that the fidelity constraint required a perceptual model that allowed the embedded watermark signal to be locally varied in response to the local properties of the corresponding cover Work. Many watermarking systems have been developed that employ a variety of perceptual models and they are generally superior to algorithms with no such models. These perceptually based watermarking embedders were early forms of informed embedding, since the added watermark signal is dependent on the cover work.

IV. SOURCE CODING AND SPIHT ALGORITHM

SPIHT means Set partitioning In Hierarchical Trees. It is an image compression algorithm that explodes the inherent similarities across the sub bands in a wavelet decomposition of an image. SPIHT is computationally very fast and among the best compression algorithms know today. According to the analysis of statistics the output binary stream of SPIHT encoding, purpose a simple and effective method combine with Huffman encode for further compression. One of the most efficient algorithms in the area of image compression is the Set Partitioning In Hierarchical Trees (SPIHT). In essence it uses a sub-band coder, to produce a pyramid structure where an image is decomposed sequentially by applying power complementary low pass and high pass filters and then decimating the resulting images. These are one-dimensional filters are applied in cascade (row then column) to an image where by creating four-way decomposition: LL (low pass then another low pass), LH (low pass then high pass), HL (high and low pass) and finally HH (high pass then high pass). There exists a spatial relationship among the coefficient at different levels and frequency sub-bands in the pyramid representation has four direct insignificant type of descendant bits type as off-springs(typeB)are utilized at locations: (1)(,) {(2,2), (2,21), (21,2), (21,21)} ijijijijij=+++O. And each of them recursively maintains a spatial similarity to its corresponding four off-spring. The SPIHT algorithm takes advantage of the spatial similarity present in the wavelet coefficient that is significant by means of a binary search algorithm. Using this source coding technique compression of the datas are carried out with respect to the input data bits . These datas are filtered with the usage of low to high pass filter,low to low filter, high to low filters etc. Which are used for processing in the next step. Thus the compression of the corresponding data streams are carried out.In the case of source coding the compression operation having a significant role to change the size of the whole data bits, It is due to improve the performance of corresponding system, it is implemented in the initial stage. Wavelet decomposition is carried out as a step of compression operation. The SPIHT algorithm sends the top coefficient in the pyramid structure. That is performed

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

using a progressive transmission scheme. It allows obtaining a high quality version of the original image from the minimal amount of transmitted data. By many research that the progressive transmission can be significantly reduced the Mean Square Error (MSE) distortion for every bit-plane, which is sending. The Discrete Wavelets Transform (DWT), which transforms a discrete time signal to a discrete wavelet representation. The steps involves is to discrete the wavelet parameters, which is used to reduce the previously continuous basis set of wavelets to a discrete and orthogonal/orthonormal set of basis wavelets.

$$\psi_{m,n}(t) = 2^{m/2}\,\psi(2^{m}t - n);\ m, n \in Z \qquad (3.1)$$

such that $-\infty < m,n < \infty$

To take advantage of the spatial relationship among the coefficient at different levels and frequency bands, the orders of the wavelets coefficient according to the significance test defined as follows:

$$\max_{(i,j)\in\tau_m} \left|c_{i,j}\right| \geq 2^{n} \qquad (3.2)$$

Where the terms are, c means wavelet coefficient at the nth bit plane, at location (i, j) of the, ,ijmτ subset of pixels, representing a parent node and its children. If the result of the significance test is YES an S flag is set to 1indicating that a particular test is significant. Suppose if the answer is NO, then the S flag is set to 0, and that coefficient is insignificant. Wavelets coefficients which are not significant at the nth bit-plane level may be significant at (n-1) the bit-plane or lower. This information is arranged in three separate lists according to the significance, they are List of Insignificant Sets (LIS), the List of Insignificant Pixels (LIP) and the List of Significant Pixels (LSP). List of Insignificant Pixels(LIP) having the condition that C(i,j) ≥2n List of Tree Roots of Insignificant Descendant Sets(LIS) having the condition that D(i,j) ≥ 2n and which is included in the type A, Insignificant Descendant of Off-spring Sets, L(i,j)=D(i,j)-O(i,j).Which having the condition that L(i,j) ≥ 2n.Which are the sub divisions of conditions to find out the coefficients having highly significance.After that the last part is known as LSP(Least Significant Pixels) having only the significant bits.The total number of source coded bits are taken as n_s.

V. CHANNEL CODING AND RS ALGORITHM

The output from the source coding is the compressed data bits. Which are transferred to the channel coding for two divisions of permutations and taken as P1 and P2. P1 is carried out before channel coding and P2 is after it. The keys are respectively taken as k1 and k2. Keys are used in the random based. And Reed Solomon (RS) code is used for generating each code word from receiving data streams from first permutation level. Reed-Solomon codes are block-based error correcting codes with a wide range of applications in digital communications and storage. The Reed-Solomon encoder takes a block of digital data and adds extra redundant bits. Errors occur during transmission or storage for a number of reason. Reed Solomon codes are a subset of BCH codes and are linear block codes. A Reed-Solomon code is specified as RS(n,k) with s bit symbols. This means that the encoder takes k data symbols of s bits each and adds parity symbols to make an n symbol code word. There are n-k parity symbols of s bits each. A Reed-Solomon decoder can correct up to t symbols that contain errors in a code word, where 2t = n-k. Reed-Solomon codes are based on a specialist area of mathematics known as Galois fields or finite fields. A finite field has the property that arithmetic operations (+,-,x,/ etc.) on field elements always have a result in the field.

A Reed-Solomon encoder or decoder needs to carry out these arithmetic operations. These operations require special hardware or software functions.A Reed-Solomon code word is generated using a special polynomial. All valid code words are exactly divisible by the generator polynomial. The general form of the generator polynomial is:

$$g(x)=(x-a^{i})(x-a^{i+1})\ldots\ldots(x-a^{i+2t}) \qquad (4.1)$$

and the code word is constructed using:

$$c(x) = g(x).i(x) \qquad (4.2)$$

where g(x) is the generator polynomial, i(x) is the information block, c(x) is a valid code word and a is referred to as a primitive element of the field.Which having channel coded output as the combination of the source coded bits and permutated bits such as,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

$$n_c = n_s + n_p \quad (4.3)$$

where, n_c is channel coded bits, n_s is source coded bits, n_p is permutated bits and also having the rate(R) as the ratio of n_s as well as n_c .Which is given as,

$$R=k/n=n_s/n_c \quad (4.4)$$

Which gives the rate about R = 2/3,In which number of source coded bits as n_s = 1bpp & n_c = 2bpp

VI. ENCRYPTED WATERMARKING

In which watermarking algorithm is used to generate encrypted watermarking data bits. From the source coding and channel coding parts data bits compression and encryption are carried out. The encrypted data bits from the channel coding block will transfer to the watermark embedding system. Hash bits or signature is used to generate the watermarking bits as well as encrypted bits from the channel coding are used for watermarking process. The reference bits also be added with the watermarking processed data bits without processing it.

$$n_w = n_c + n_h + n_m \quad (5.1)$$

Additional MDHTR and Book keeping matrix also be included with this reference bits separately. Here, n_c is channel coded bits and utilizing for generating encrypted watermarking image. Which having the size about 1.5bpp and include n_s as well as n_p. Each of them having the size about 1bpp and .5bpp respectively. Hash bits having the size about .5bpp. Which is combined with n_c and form, 2bpp of data. Which is utilized for water marking and the reference bits n_m is embedded with the watermarked image and resultant get as totally as the output as 8bpp of size. Which is generally known as encrypted watermarked image, n_w. Thus watermarking can be done and processed datas having the ability to provide the extreme level of security over the data recovering by the intruder. The representation of the n_w bits can be considered as follows as the combination of channel coding bits, hash bits or check bits and reference bits. Which are given as,Where, n_w is the watermarked image, n_c is the channel coded bits, n_s is the source coded bits, n_p permutated bits, n_h is the hash bits, n_m is the reference bits Thus the corresponding input image is compressed and encrypted using different coding techniques such as source coding as well as channel coding and after that watermarking is done using hash bits and encrypted data bits. The resultant image must be the combination of encrypted watermarking as well as reference bits.

VII. EXPERIMENT RESULTS

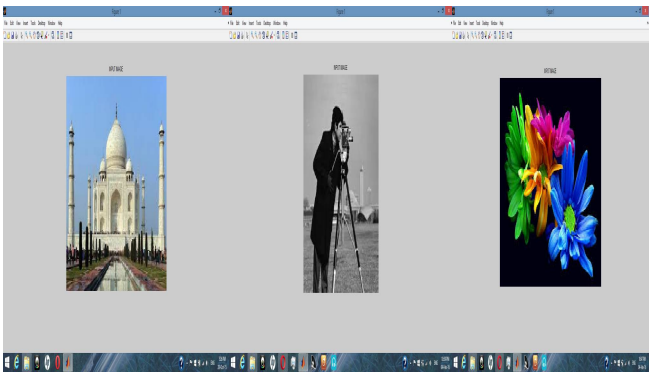

Figure 6(a) Input Images

The input images are given in figure 6(a) for generating encrypted watermarking images. In this set the images having the different grayscale levels with the direct view. Thus the characteristics are different one without any kinds of doubts. It is clear that the output encrypted watermarked images are absolutely different in pattern of setting through various steps. Those processed images are provided in the following contents according the step wise manner. Which are given in this order of compression stage as well as final stage.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

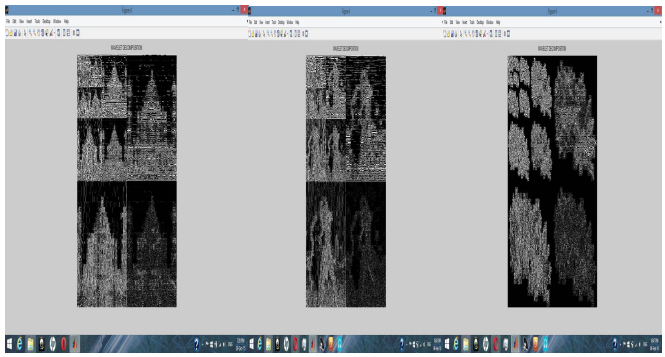

Figure 6(b) Compression using DWT

The compression of the images are carried out in the next step and it is an important step in the watermarking scheme. Which can be considered in the figure 6(b). Compression is carried out with the support of encoding as well as Discrete Wavelet Transform. Thus compression of the corresponding image is carried out.

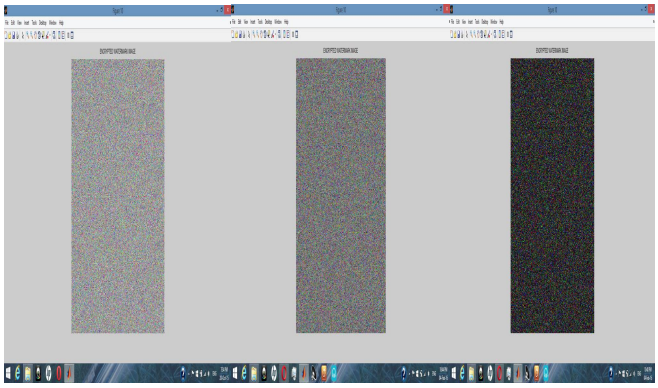

Figure 6(c) Encrypted Watermarks of Input images

After that the Watermarking Bits, Encryption Bits and reference bits are generated. Which are embedded at the final step and generate the required encrypted watermark images in figure 6(c). Each of the images having different kinds of patterns based on the gray scale levels variations in different images. Which is the protected format of the corresponding images.

VIII. **CONCLUSION**

Security over the data transmission in the case of image is an important concept. In which mainly watermarking is utilizing to make changes over the images and encryption is used to provide more protection. In the proposed method advanced encrypted watermarking is used to provide extra protection. In each step, Protection is allotted. When compare to old methods,watermark is allowing image's noised view. Which is the important difference of proposed method from existing methods. In old approaches, image can be understood from that encrypted one. But in this scheme encrypted watermark mask the whole data and we can not understand the original one. So recovering datas by an intruder is not possible. In which encrypted watermark image is generated systematically. Additionally MDHTR, Encryption, Reference embedding and Watermark generation using Hash bits are done successively. The future scope is detecting the corresponding encrypted watermark image and recover it with the tamper detection and performance analysis. Which is applicable in secure data transmission mainly in the form of images.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

IX. FUTURE WORK

The future scope is detecting the corresponding encrypted watermark image and recover it from the watermarked data bits.Also the tamper detection can be found out using that section in systematic manner. Which is useful to determine the tolerable tampering rate as well as mean square error values for different images. Using these parametric concepts, overall comparison can be carried out in the different strategies such as efficiency and performance analysis. Using these ideas, images and its processing and recovering time duration are considered to valuate it with old approaches. Thus the real impact of this system can be revealed successively. According these concepts and overview, which can be proved that it is suitable in secure data transmission mainly in the form of images. So the important aim to determine the tampered regions in an image and recover the original image from the noised data as similar as in the exact image. Tampering recovery rate will also be improved in the future with proper tolerable tampering rate. Also overcome the chance of occurance of errors over the image processing. Which are the important future views about this work.

REFERENCES

[1] Bai, Zhengyao, and Dimitrios Hatzinakos. "LBP-based biometric hashing scheme for human authentication." In *Control Automation Robotics & Vision (ICARCV), 2010 11th International Conference on*, pp. 1842-1847. IEEE, 2010.
[2] Boubiche, Djallel Eddine, Sabrina Boubiche, and Azeddine Bilami. "A Cross-layer Watermarking-based Mechanism for Data Aggregation Integrity in Heterogeneous WSNs." IEEE(2015).
[3] Castiglione, Arcangelo, Alfredo De Santis, Raffaele Pizzolante, Aniello Castiglione, Vincenzo Loia, and Francesco Palmieri. "On the Protection of fMRI Images in Multi-Domain Environments." IEEE,2015.
[4] Chaluvadi, Surya Bhagavan, and Munaga VNK Prasad. "Efficient image tamper detection and recovery technique using dual watermark." In *Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress on*, pp. 993-998. IEEE, 2009.
[5] Chetan, K. R., and Nirmala Shivananda. "A new fragile watermarking approach for tamper detection and recovery of document images." In *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*, pp. 1494-1498. IEEE, 2014.
[6] Jamil, Nighat, and Arshad Aziz. "A unified approach to secure and robust hashing scheme for image and video authentication." In *Image and Signal Processing (CISP), 2010 3rd International Congress on*, vol. 1, pp. 274-278. IEEE, 2010.
[7] Li, Yuenan, Zheming Lu, Ce Zhu, and Xiamu Niu. "Robust image hashing based on random Gabor filtering and dithered lattice vector quantization."*Image Processing, IEEE Transactions on* 21, no. 4 (2012): 1963-1980.
[8] Liu, Ruyu, Guodong Wang, Ping Wang, and Wei Huang. "An image authentication scheme based on sliding window." In *Control and Decision Conference, 2008. CCDC 2008. Chinese*, pp. 2937-2940. IEEE, 2008.
[9] Lu, Wenjun, and Min Wu. "Multimedia forensic hash based on visual words." In*Image Processing (ICIP), 2010 17th IEEE International Conference on*, pp. 989-992. IEEE, 2010.
[10] Lv, X., & Wang, Z. J. (2008, October). Fast Johnson-Lindenstrauss transform for robust and secure image hashing. In *Multimedia Signal Processing, 2008 IEEE 10th Workshop on* (pp. 725-729). IEEE,2008
[11] Mall, Vinod, Kedar Bhatt, Suman K. Mitra, and Anil K. Roy. "Exposing structural tampering in digital images." In *Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on*, pp. 1-6. IEEE, 2012.
[12] Prungsinchai, Supakorn, Fouad Khelifi, and Ahmed Bouridane. "Sub-images based image hashing with non-negative factorization." In *Electronics, Circuits and Systems (ICECS), 2012 19th IEEE International Conference on*, pp. 781-784. IEEE, 2012.
[13] Roy, Sujoy, and Qibin Sun. "Robust hash for detecting and localizing image tampering." *Image Processing, 2007. ICIP 2007. IEEE International Conference on*. Vol. 6. IEEE, 2007.
[14] Tagliasacchi, Marco, Giuseppe Valenzise, and Stefano Tubaro. "Hash-based identification of sparse image tampering." *Image Processing, IEEE Transactions on* 18, no. 11 (2009): 2491-2504.
[15] Tashk, Ashkan, Habibollah Danyali, and Mohammad Ali Alavianmehr. "A modified dual watermarking scheme for digital images with tamper localization/detection and recovery capabilities." In *Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on*, pp. 60-65. IEEE, 2012.
[16] Wu, Min, Yinian Mao, and Ashwin Swaminathan. "A signal processing and randomization perspective of robust and secure image hashing." *Statistical Signal Processing, 2007. SSP'07. IEEE/SP 14th Workshop on*. IEEE, 2007.
[17] Zhan, Rui-Xin, K. Y. Chau, Zhe-Ming Lu, Bei-Bei Liu, and W. H. Ip. "Robust image hashing for image authentication based on DCT-DWT composite domain." In *Intelligent Systems Design and Applications, 2008. ISDA'08. Eighth International Conference on*, vol. 2, pp. 119-122. IEEE, 2008.
[18] Zhang, Xinpeng, and Shuozhong Wang. "Fragile watermarking with error-free restoration capability." *Multimedia, IEEE Transactions on* 10, no. 8 (2008): 1490-1499.
[19] Zhang, Xinpeng, Shuozhong Wang, Zhenxing Qian, and Guorui Feng. "Reference sharing mechanism for watermark self-embedding." *Image Processing, IEEE Transactions on* 20, no. 2 (2011): 485-495.
[20] Zhu, Ting-ting, Dong-hui Hu, and Li-na Wang."Perceptual Hash Functions Based on Contourlet Transform and Singular Value Decomposition." In*Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*, vol. 2, pp. 87-90. IEEE, 2009.