International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Survey on Data Hiding in Encrypted Images

Aniket Kesharwani[1] , Hemant Gupta[2]

[1] *Student, Dept of CSE , R.I.T Indore M.P*

[2] *Assistant Professor, Dept of CSE R.I.T Indore M.P*

Abstract: - As the use digital techniques for transmitting and storing images are increasing; it is becoming an important issue how to protect the confidentiality, integrity and authenticity of images. So one solution of these things is to hide our valuable information in encrypted image. In this paper we make a survey of different data hiding methods. Here we first describe the purposes for image hiding, then data hiding in encrypted images.

Keywords: - Information Hiding, Encryption decryption, Reversible data hiding.

Introduction: - With the popularity of computers and Internet, data is commonly transformed into digital forms and transmitted on Internet. Digitized data can be texts, images, audios or videos. A problem arose from sending digital data on Internet is how to ensure the secrecy of data transmission. Any modification of digital data makes it hard to protect the security of digital data.
Consequently we know that digital data can also be transmitted through data communication networks without losing quality in a fast and inexpensive way. With digital multimedia, distribution over World Wide Web Intellectual Property Right (IPR) is more threatened than ever due to the possibility of unlimited copying. So by using some encryption techniques this easily copying of the data need to be restricted. However encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. This problem can be solved by hiding some ownership data into the multimedia data which can be extracted later to prove the ownership. This technique mostly used in bank currency where a watermark is embedded which is used to check the originality of the note. The same concept called watermarking may be used in multimedia digital contents for checking the authenticity of the original content.

Simple Module for Cryptography or Encryption: -

A technique in which secret messages are transferred from one person to another over the communication line called cryptography. The technique(s) used to convert the original data into secret code or data is called data encryption technique for all kinds of data such as textual data, Image data or multimedia data for secured communication over a network. In this paper we focus on Image encryption which has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication; etc. Images encryption is different from the simple data encryption. So in general the data hiding in image involves four steps.

1. Selection of the secret media where the data will be hidden.
2. The undisclosed message or information that is needed to be masked in the cover image.
3. A function that will be used to hide the data in the cover media and its inverse to retrieve the hidden data.
4. An optional key or the password to authenticate or

To hide and unhide the data. Based on above encryption standard a process of Non separable reversible data hiding in encrypted image is as shown in Fig.1.where A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the data extraction is not separable from the content.

© 2015, IRJET.NET- All Rights Reserved

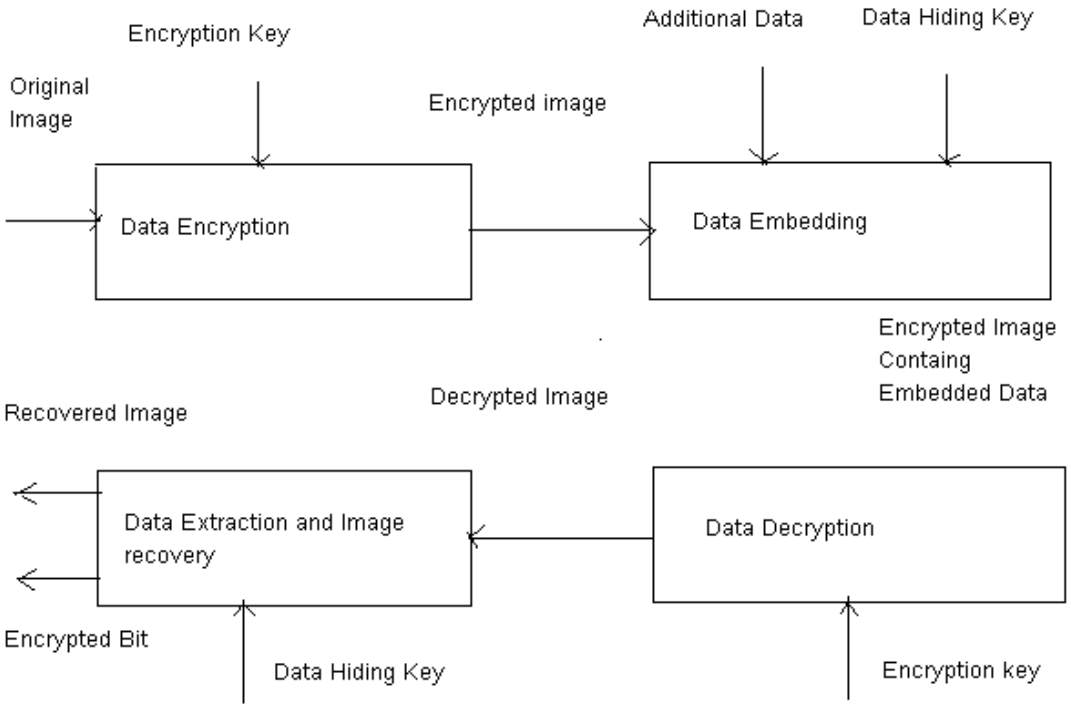

Fig. 1: Non separable reversible data hiding in encrypted image

Now a days when more and more sensitive information is stored on computers and transmitted over the Internet for which security and safety of information need to be ensured as image is also an important part of that sensitive data. Therefore it's very important to protect these images from legitimate users. There are many novel reversible data hiding scheme for encrypted image available which are made up of image encryption, data embedding and data-extraction/image-recovery phases. In which the data of original cover are entirely encrypted and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered. Some of the methods are discussed in next section.

This paper is organized as follows in introduction Section general guidelines about cryptography and encryption. In Section 2 literature review on existing research paper. Finally conclusion in section 3.

b) Applications of Data Hiding

a. Secret communication.

b. Image authentication for IPR.

c. Fingerprinting (traitor-tracing).

d. Adding captions to images, additional information, such as subtitles, to videos

e. Image integrity protection (fraud detection).

f. Copy control in DVD.

g. Intelligent browsers, automatic copyright.

h. information, viewing movies in given rated version.

c) Properties of hiding schemes

I. Robustness

The embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition. Examples are linear and nonlinear filters (blurring, sharpening, median filtering), lossy compression, contrast adjustment, gamma correction, re coloring, re sampling, scaling, rotation, small nonlinear deformations (as in Stir Mark [Kuh1]), noise

© 2015, IRJET.NET- All Rights Reserved

adding, cropping, printing / copying / scanning, D/A and A/D conversion, pixel permutation in small neighborhood, color quantization (as in palette images), skipping rows / columns, adding rows / columns, frame swapping, frame averaging (temporal averaging), etc. We emphasize that robustness does NOT include attacks on the embedding scheme that are based on the knowledge of the embedding algorithm or on the availability of the detector function. Robustness means resistance to "blind", non-targeted modifications, or common image operations.

II. Un-Detestability

Impossibility is to prove the presence of a hidden message. This concept is inherently tied to the statistical model of the carrier image. The ability to detect the presence does not automatically imply the ability to read the hidden message. Un-detectability should not be mistaken for invisibility.

III. Invisibility

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not. A commonly accepted experimental arrangement (so called blind test) frequently used in psycho-visual experiments is based on randomly presenting a large number of carriers with and without hidden information and asking the subjects to identify which carriers contain hidden information. Success ratio close to 50% demonstrates that the subjects cannot distinguish carriers with hidden information. We note that the concept of invisibility could be defined in other manners leading to more or less strict concepts. The test described above is really a test for visibility of artifacts caused by data embedding schemes. If the visibility of artifacts was tested by presenting both covers (those that do contain hidden information and those that do not) at the same time side by side, a stricter concept of invisibility would result.

IV. Security

The embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message.

V. Un-Detectability

This property is typically required for secure covert communication. We say that the embedded information is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For example, if a steganography method uses the noise component of digital images to embed a secret message, it should do so while not making statistically significant changes to the noise in the carrier. The concept of un-detectability is inherently tied to the statistical model of the image source. If an attacker has a more detailed model of the source, he may be able to detect the presence of a hidden message. Note: the ability to detect the presence does not automatically imply the ability to read the hidden message. We further note that un-detectability should not be mistaken for invisibility a concept tied to human perception.

II. LITERATURE SURVEY

Wei Liu et al. [1] in this proposal, resolution progressive compression scheme is used which compresses an encrypted image progressively in resolution, such that the decoder can observe a low resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. The encoder starts by sending a down sampled version of the cipher text. At the decoder, the corresponding low-resolution image is decoded and decrypted, from which a higher-resolution image is obtained by intra-frame prediction. The predicted image, together with the secret encryption key, is used as the side information (SI) to decode the next resolution level. This process is iterated until the whole image is decoded. So this multi-resolution approach makes it possible to have access to part of the spatial source data to generate more reliable spatial and temporal side information. But there is need to increase the efficiency of overall data compression to avoid the loss of any kind of data.

W. Puech et al. [2] proposed an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step for protection of multimedia based on Encryption and watermarking algorithms rely on the Kirchhoff's principle, all the details of the algorithm are known, and only the key to encrypt and decrypt the data should be secret. The first one is when there is homogeneous zones all blocks in these zones are encrypted in the same manner. The second problem is that block encryption methods are not robust to noise. Indeed, because of the large size of the blocks the encryption algorithms per block, symmetric or asymmetric cannot be robust to noise. The third problem is data integrity.

The combination of encryption and data-hiding can solve these types of problems hence by using this approach a reversible data hiding method for encrypted images is able to embed data in encrypted images and then to decrypt the image and to rebuild the original image by removing the hidden data but it is not possible to use when high capacity reversible data hiding method for encrypted images.

© 2015, IRJET.NET- All Rights Reserved

Christophe Guyeux et al. [3] developed a new framework for information hiding security, called chaos security. In this work, the links among the two notions of security is deepened and the usability of chaos-security is clarified, by presenting a novel data hiding scheme that is twice stego and chaos-secure. The aim of this approach is to prove that this algorithm is stego-secure and chaos-secure, to study its qualitative and quantitative properties of unpredictability, and then to compare it with Natural Watermarking. Some of the probabilistic models are used to classify the security of data hiding algorithms (Runge-Kutta algorithm) in the Watermark Only Attack (WOA) framework. Hence method possesses the qualitative property of topological mixing, which is useful to withstand attacks but cannot be applied in KOA and KMA (Known Message Attack) setup due to its lack of expansively schemes which are expansive.

Mark Johnson et al. [4] proposed the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. In this method first data encryption is used and then the encrypted source is compressed but the compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data without any knowledge of the original source. At first glance, it appears that only a minimal compression gain, if any, can be achieved, since the output of an encrypt or will look very random. However, at the receiver, there is a decoder in which both decompression and decryption are performed in a joint step. In a broad spectrum in this approach, the encrypted data can be compressed using distributed source-coding principles as the key will be available at the decoder but in some cases the possibility of first encrypting a data stream and then compressing where compressor does not have knowledge of the encryption key.

Jun Tian et al. [5] proposed reversible data embedding which is also called lossless data embedding which embeds invisible data into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. A captivating feature of reversible data embedding is the reversibility i.e. one can remove the embedded data to restore the original image. A common approach of high capacity reversible data embedding is to select an embedding area for suppose; the least significant bits of some pixels in an image and embed both the payload and the original values in this area needed for exact recovery of the original image into such area. Here DE (difference expansion) technique which discovers extra storage space by exploring the redundancy in the image content as well, DE technique employed to reversibly embed a payload into digital images. The main significance of this method is the payload capacity limit and the visual quality of embedded images but if there is reversible data embedding then it is a fragile technique because when the embedded image is manipulated and/or lossy compressed the decoder will find out it is not authentic and thus there will be no original content restoration.

PatrizioCampisi et al. [6] present a novel method to blindly estimate the quality of a multimedia communication link by means of an unconventional use of digital fragile watermarking. Data hiding by digital watermarking is usually employed for multimedia copyright protection, authenticity verification, or similar purposes. Watermarking is here adopted as a technique to provide a blind measure of the quality of service in multimedia communications. The general watermark embedding procedure consists of embedding a watermark sequence which is usually binary into host data by means of a key. In the detection phase the key is used to verify the presence of the embedded sequence. With regard to the domain where the watermark embedding occurs which can distinguish methods operating in the spatial domain, DCT domain, Fourier transform domain and in the wavelet transform domain and it allows one to blindly estimate the Quos provided by a coder/channel system without affecting the quality of the video-communications but has complexity of the Quos evaluation procedure appears negligible in comparison with MPEG-2/4 decoding and adaptive on-board array processing.

StephaneBounkong et al. [7] approach can be used on images, music or video to embed either a robust or fragile watermark. In the case of robust watermarking the method shows high information rate and robustness against malicious and no malicious attacks, while keeping a low induced distortion. This method is based on related to a least significant bit modification in the ICA domain. ICA allows the maximization of the information content and minimization of the induced distortion by decomposing the cover text (in this case the image) into statistically independent sources. Embedding information in one of these independent sources minimizes the emerging cross-channel interference. In fact, for a broad class of attacks and fixed capacity values, one can show that distortion is minimized when the message is embedded in statistically independent sources, this extremely simple transformation facilitates the use of Bayesian decoding techniques. As this method is based on embedding information using statistically independent sources the same watermarking method can be easily applied across different media but it needs additional security in the use of specific mixing/demising matrices that are not easy to obtain.

© 2015, IRJET.NET- All Rights Reserved

G. Boato et al. [8] presents a novel method for the secure management of digital images formulated within the mathematical theory of polynomial interpolation as main pioneering features. This work is based on a hierarchical joint ownership of the image by a trusted layered authority and on a deterministic watermarking procedure, embedding a short meaningful or random signature into the image. To show the results here the signature written in English alphabet is first translated into a sequence of integers by means of a look-up table. Such a sequence of integers is used to set the coefficients of a trigonometric polynomial from which a predefined number of samples is extracted evaluated at equally spaced points. Finally, the values of the samples are embedded into the lowest frequency coefficients of the original image transformed into the DCT domain excluding the DC component a high performance is obtained in terms of false detection even in critical situations or reasonable amount of image degradation due to the image processing operators such as filtering, geometric distortion(s) and compressions but hierarchical scheme is not controlled by the kind of watermarking technique adopted due to which it is prone to the malicious attacks. Hence need to have more constructive and robust techniques to avoid such attacks. Abd-el-Kader H. Ouda et al. [9] proposed the Work for security of Wong's technique is vulnerable to cryptographer's attacks. This is due to the use of short keys in the public-key cryptosystem. Short keys are used in Wong's technique to make the watermark small enough to fit in an image block. A new method of applying the cryptographic hash function is utilized. This method makes the image blocks able to hold longer and secure watermarks while providing similar level of the localization accuracy. Here they utilized MD5 algorithm to achieve a high-level of localization accuracy but the security flaws of MD5 are predefined hence known to all due to which it is prone to the wear security attacks contemplating to the non-reliability.

G. Boato et al. [10] proposed a novel method for steganography image watermarking with two main innovative features i.e., it involves a hierarchical control, committing the watermark reconstruction to a trusted layered authority and it is deterministic, embedding ashort meaningful signature into the cover image. In this method they took a signature written in English alphabet and translated it into a sequence of integers with suitable look up table. Next, they identified it with the coefficients of a trigonometric polynomial and embed a redundant number of samples of the polynomial evaluated at equally spaced points into the lowest frequency coefficients of the DCT matrix excluding the DC component. In general by using this method it is possible that the embedded signature can be accurately recovered even in presence of a reasonable amount of image degradation due to image processing operators but it has no chance to resist against the attack byinserting multiple watermarking.

HuipingGuo et al. [11] proposed a novel procedure that makes use of a generalized secret sharing scheme in cryptography to address the problem of image watermarking. In this scheme, given that multiple owners create an image jointly distinct keys are given to only an authorized group of owners so that only when all the members in the group present their key scan the ownership of the image be verified. This process is based on generalized secret sharing scheme, multiple watermarks, one for each owner's key and one for the secret key are embedded so that both full ownership and partial ownership can be verified. Spread spectrum watermarking schemes, quantization watermarking schemes usually quantize the values of host images spatial domain or in the spectrum domain to a pre specified set of values according to binary watermarking bits. Thus, the watermark information is completely contained in the watermarked images and the watermarking detector can detect the embedded watermark blindly. By using this scheme they achieved two important outcomes

1. Access structure is more flexible under a secret sharing scheme. If a secret sharing scheme is not spatially multiplexed into the image, we have no way to control the authorized set in which participants can jointly verify ownership.

2. Secondly the secure secret-based watermark is embedded to establish a secure connection between owners. But due to multiple watermarking there is possibility of loss of data due to which the watermarked image may be distorted affecting the original data.

F. Cerou, et al. [12] discusses a novel strategy for simulating rare events and an associated Monte Carlo estimation of tail probabilities. This method uses a system of interacting particles and exploits a Feynman- Kac representation of that system to analyze their fluctuations. This precise analysis of the variance of a standard multilevel splitting algorithm reveals an opportunity for improvement. This work proposes a similar algorithm including the use of quantities of the random variable on the swarm of particles in order to estimate the next level. The main difference is their two stage procedure they first run the algorithm just to compute the levels and then they restart from the beginning with these proposed levels. Actually in this method it is shown that by computing the levels on the fly within the same run as the one to compute the rare event probability paid a small bias on the estimate. They mainly claim that from a practical point of view one should favor the variants without bias in

© 2015, IRJET.NET- All Rights Reserved

the desired estimates but for security reason anti-collusion codes have yet to be employed. Frank

Hartung et al. [13] proposed a method for watermarking of images and video based on idea(s) from spread spectrum radio communications namely additive embedding of a signal adaptive or non-adaptive pseudo-noise watermark pattern, and watermark recovery by correlation. In this process the water mark bits are embedded with the spread information bits and then modulated with a crypto logically secure pseudo noise signal, scaled according to visibility criteria and added to the image or video pixels. The complexity of watermarked bits and the spread information improves resistance against the simple attacks, detection-disabling attacks, ambiguity attacks and removal attacks but there is no watermarking system can guarantee absolute security.

Saraju P.Mohanty et al. [14] proposed ascheme of digital watermarking for both gray and color images in which a visible and invisible signal watermarkis embedded in a multimedia document for copyright protection. In visible watermarking of images a secondary is embedded in a primary image such that watermark is intentionally observable to a human observer. In this technique the modification of the gray values of host image is based on its local as well as global statistics. Whereas in the case of invisible watermarking the embedded data is not perceptible but used and each owner embeds his watermark may be extracted by using some simple computer program(s).The invisible watermarking uses logical operation instead of simple a addition. However due to the visible signals though it is called robust method but can be tampered using various software.

Mohan S Kankanhalli et al. [15] proposed a novel invisible and robust watermarking technique for images including video data. Here they proposed a new way of analyzing the noise sensitivity of every pixel based on the local region image content such as texture, edge and luminance information and it can be done either embedded in the spatial domain or can beDCT coded to be embedded in the transform domain has a JPEG standard. By transforming spatial data into another domain such as spatial frequency statistical independence between pixels as well as high-energy compaction can be obtained. The general method of DCT coding involves dividing the original spatial image into smaller N x N blocks of pixels, and then transforming the blocks to obtain equal-sized blocks of transform coefficients in the frequency domain. These coefficients are then threshold and quantized in order to remove subjective redundancy in the image. In all this method I based on human visual system (HVS) and can be applied to transform domain techniques but it is not very robust against rotation and scaling attacks.

Kede Ma et al. proposed reversible data hiding in encrypted images by reserving room before encryption method for data hiding in encrypted image. Reversible data hiding (RDH) in encrypted images is able to maintain the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest.

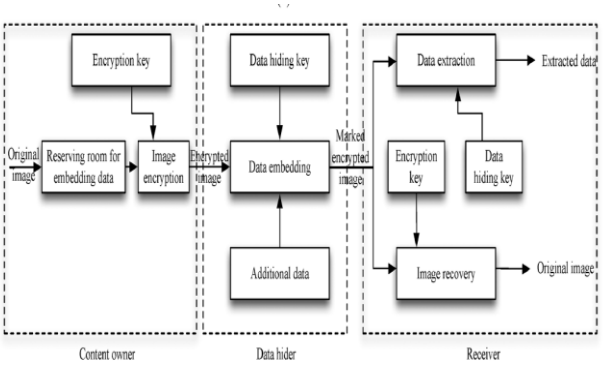

Fig. 1 Illustration of Reversing Data Hiding Steps.

In above figure steps of reversible data hiding method with encrypted image is illustrate, in which instead of popular vacating room after encryption method we use reversible data hiding method.

Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into three steps:

a) IMAGE PARTITION,
b) SELF REVERSIBLE EMBEDDING followed by image encryption.

At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

a) IMAGE PARTITION

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition.

b) SELF REVERSIBLE EMBEDDING

The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH

© 2015, IRJET.NET- All Rights Reserved

algorithms. We simplify the method in to demonstrate the process of self-embedding.

Data Hiding In Encrypted Image

In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or unauthorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

Data Extraction and Image Recovery

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

Data Extraction and Image Restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image.

III. CONCLUSION

This survey paper gives the detail analysis of data hiding using image encryption based on image. But due the visibility problems it is possible to tamper some sensitive by the simple attacks, detection disabling attacks, ambiguity attacks or removal attacks. Hence there is need of some constructive, robust secured method of data hiding in encrypted image which we would be trying in future course of our dissertation work.

REFERENCES

[1]. Wei Liu, WenjunZeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 – 1102.

[2]. W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for EncryptedImages", SPIE, IS & T'08: SPIE Electronic Imaging, Security, Forensics, Steganography And Watermarking of Multimedia Contents, San Jose, CA, USA.

[3]. Christophe Guyeux, Nicolas Friot, and Jacques M. Bahi, "Chaotic iterations versus Spread-spectrum: chaos and stego security", January 25-2011, IIHMSP,pp. 208-211.

[4]. M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramchandran, "On compressing and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[5]. J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[6]. PatrizioCampisi, Marco Carli, Gaeta no Giunta and Alessandro Neri, "Blind Quality Assessment System for Multimedia Communications using Tracing Watermarking" IEEE Transactions on Signal Processing, Vol 51, No 4, Apr 2003, pp. 996 – 1002.

[7]. S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images," Journal of Machine Learning Research, vol. 1, pp. 1–25, 2002.

[8]. G. Boatoa, F.G.B.DeNatalea, C. Fontana rib, F. Melgania"Hierarchical ownership and deterministic watermarking of digital images via polynomial interpolation", Signal Processing: Image Communication 21 (20 0 6), pp. 573–585.

[9]. A.H. Ouda, M.R. El-Jakka, "A practical version of Wong's watermarking technique", Proc. ICIP (2004) 2615–2618.

[10]. G. Boato, C. Fontanari, and F. Melgani "Hierarchical deterministic image watermarking via polynomial interpolation" Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept-2005,

[11]. H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems 9 (3) (2003) 249–

[12]. Frederic Cerou, Pierre Del Moral, Teddy Furon and Arnaud Guyader, "Sequential Monte Carlo for rare event estimation" Statistics and Computing, pp. 1– 14, 2011.

[13]. F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counter attacks", Proc. SPIE, vol. 3657, pp. 147–158, Jan. 1999.

[14]. Mohanty S, Ramakrishna KR (1999) A dual watermarking technique for images." Proceedings of ACM Multimedia 1999, Orlando, 30 October–5 November 1999, pp 49–51.15.

[15]. M. Kankanahalli, et al., "Content Based Watermarkingfor Images", Proc. 6th ACM InternationalMultimedia Conference , ACM-MM 98, Sep. 1998, Bristol, UK, pp.61 - 70.

© 2015, IRJET.NET- All Rights Reserved