International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Review of Reversible Data Hiding Techniques

Harshila Gawali [1], Prof.R.C. Samant [2]

[1] *ME(CSE) Student, Gokhale Education Society's, R. H. Sapat College of Engg, Nashik, Maharashtra, India*

[2]*Assistant Professor ME Computer Engineering Gokhale Education Society's, R. H. Sapat College of Engg, Nashik, Maharashtra, India-422003.*

Abstract - ***Reversible data hiding is a technique by using which we can embed essential data into images, audio, video and so on. This system applies a method of hiding data in an image and video by reserving room before encryption. The proposed scheme increases the amount of data that can be hidden in the image or video which also guarantees the lossless recovery of image or video after extraction is completed. All the previous methods of reversible data hiding were developed such that they were vacating room for data hiding after encrypting the image, which results in introduction of some error rates at the time of data extraction and image recovery. This system proposes a new method for reversible data hiding in which reserving room before encryption (RRBE) is used in images and videos using visual cryptography, so that image or video extraction will be free of any error. It is also known as new watermarking technique which is used to authenticate an image and video by embedding some data in it.***

Key Words: *RRBE, RRAE, RDH, ABE, encryption, partitioning, self reversible embedding.*

1. INTRODUCTION:

Now-a-days security is considered as most important critical factor in any communication systems. Issues in such security systems are integrity, privacy, authentication and non-repudiation, such issues must be handled carefully. Here the security goals are namely: confidentiality, availability and integrity that can be threatened by security attacks. So to protect the original information from such attacks the data hiding techniques are implemented. To maintain the security and authentication, Reversible Data Hiding i.e. RDH techniques are related to steganography and cryptography function [3]. Encryption and data hiding are two techniques of data protection. Data hiding techniques embeds original data which we don't want to disclose into cover media by introducing slight acceptable modifications, while encryption techniques converts plaintext data into unreadable form i.e. ciphertext. It is beneficial to embed the data into a digital media to communicate the secret messages. The owner can modify the original content of the media using images, so that the embedded data is hidden.[1] Encryption provides confidentiality for images and video as well as it is effective technique which converts the original and secret data to incomprehensible one.

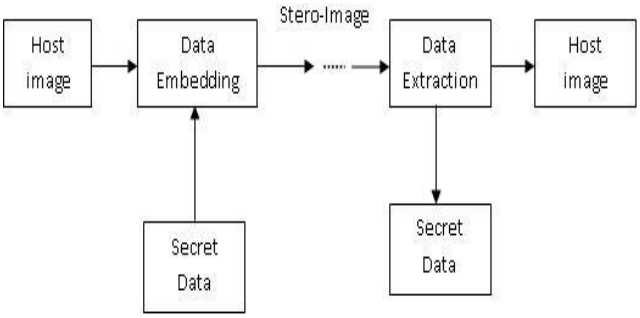

Figure 1: Block diagram of RDH

If we are able to apply RDH to encrypt image then some good applications can be generated through it.

For example: Suppose that a medical image database stored in some data center, then some notations can be embedded into the encrypted version of a medical image through a RDH technique by a server in the data center. The server can manage the image or verify its integrity by using the notations without having the knowledge of the original content. This will protect the patient's privacy. At the same time, a doctor can decrypt and restore the image for further diagnosing by using the cryptographic key.

Reversible data hiding in images or videos is a technique, by which the original content can be recovered without loss after the embedded data is extracted. This technique can be widely used in various fields such as medical, military and law forensics, where distortion of the original cover is not allowed. Reversible data hiding technique is used to embed additional data into cover media such as image or video. Recently many new RDH techniques are developed which gives a general framework for RDH. It works by first extracting the features of the original cover media and then compressing them without loss, extra space can be saved by embedding auxiliary data. All previous methods of RDH embed data by reversibly extracting room from the encrypted images, which may lead to some errors while data is being

extracted and/or image is being restored. Here a novel method with a traditional RDH algorithm by reserving room before encryption is proposed, and thus it is possible to reversibly embed data in the encrypted image and videos. Objective of this system is to achieve technique of secured transmission of highly sensitive information over the internet. Data hiding into cover media such as video is one of the challenging task compared to data hiding in images, but as videos are more secure way for embedding secure information than images, in proposed method it is possible to hide the data in videos by using public key cryptography. In this system, a novel method by reserving room before encryption with a traditional RDH algorithm is proposed.

RELATED WORK

There are various techniques which provide security that are defined following:

A. Cryptography:

Cryptography is an art of securely transferring the message from sender to receiver. It uses the key concept for encryption the message information known as cryptography. It is used when communicating over the untrusted media such as internet. Cryptography is the technique that used in securely transfers the information with the use of algorithm which is un-readable by the third-party.

B. Categories of cryptography

a) Symmetric-key cryptography:

Symmetric-key cryptography is the technique that performed encryption and decryption by using single key. It is also known as secret key encryption.

b) *Asymmetric-key cryptography*:

It is also known as the public–key cryptography. In this two keys are used, one for encryption i.e. public and another for decryption i.e. decryption.

c) Hash Encryption:

Hash encryption performed by using the hash function. It provides security to user by using this concept. It produces fixed length signature for a message.

Here our concern with image encryption. Image encryption technique is different from simple encryption.

The data hiding in image takes place following four steps that are:

- Select the medium or carrier.
- Message which needed protection.
- A function that will be used to hide data in the cover media.
- Alternative key which provide authentication.

C. Types of Image cryptography/Encryption

a) **Generation of encryption-key:** It is generated by randomly by using random function. It uses 128-bit of value.

b) **Generation of pseudo-random sequence:** It is generated by using encryption-key. For example RC-4 algorithm used to generate the pseudo random sequence using 128-bit encryption key.

D. Steganography:

Steganography word takes from Greek word that is made up of two words such as “stegan” and “graphy”, it means cover or secret writing. It deals with composing hidden messages. It is the way of hiding information without the knowledge of third-party. Steganography provides the security to the message as well as content of the information. It is an art of hiding information by embedding messages within other, seemingly harmless messages. Steganography perform using three media:

- Hiding a message inside “text”.
- Hiding a message inside “images”.
- Hiding a message inside “audio” & “video”.

It is the process of hiding a secret message within the carrier such as image, text, and audio.

E. Data hiding techniques:

Mainly the data hiding techniques are classified into two techniques:

1. Reversible data hiding technique:

In this technique the message signal as well as the original cover can be with no loss recovered simultaneously.

2. Irreversible data hiding technique:

In this technique the message signal can be recovered with no loss but the original cover can be lost. So in general reversible data hiding techniques can be used now a days. Method of reversible data hiding are reserving room before encryption and vacating room after encryption as given below:

a) Vacating Room after the Encryption:

In this method first encrypt the original image using the cipher with the encryption key. Next to this it is given to the data hider to hide some auxiliary data in it by with no loss vacating the room required for data hiding key. At receiver the content owner or an authorized third party can be extract the embedded data with the help of data hiding key and also recover the original image according to the encryption key. This method compresses the encrypted LSBs of image to vacate the room for additional data.

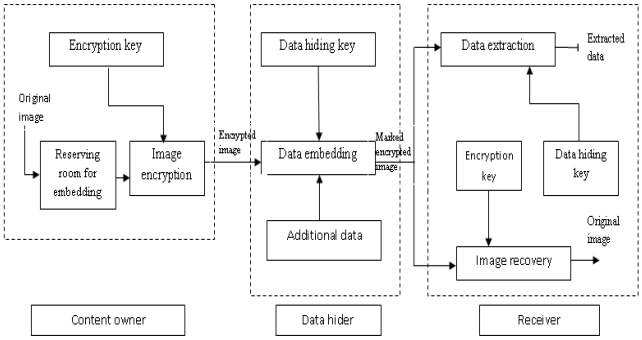

Figure 2: Vacating Room after the Encryption

a) Reserving room before the encryption:

Vacating room from the encrypted images losslessly is sometimes difficult and not efficient, so if we reverse order of encryption and vacating room, i.e., reserving room before image encryption, the RDH tasks in encrypted images would be more natural and much easier which gives the novel framework, reserving room before encryption (RRBE). [2]

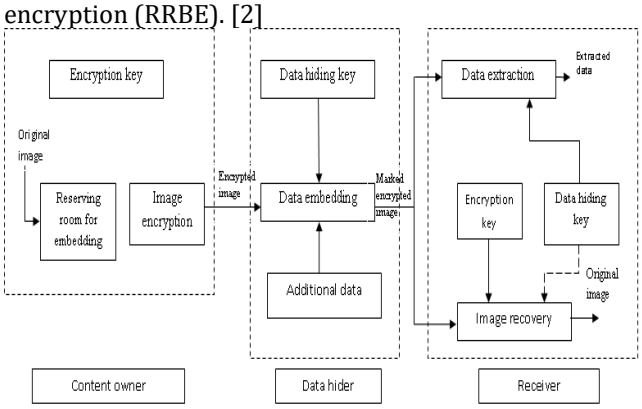

Figure 3: Vacating before the Encryption:

There are some standard RDH algorithms available which are ideal for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. [1] This is because in this new framework, follow the customary idea that first lossless compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

D. Performance analysis of a reversible data embedding algorithm:

Data embedding in the reversible manner which is the data embedding without any loss embeds the data or payload into digital image in reversible manner. After data embedding the quality of original image may be degraded which is to be avoided. The attractive property of data embedding in reversible manner is reversibility, which is after data extraction the original quality image is restored back. Reversible data embedding hides some information in a digital image in such a way that an approved party image to its original state. The presentation of a reversible data-embedding algorithm can be measured using following,

- Data embedding capacity limit
- Visual quality
- Complexity

The data without any distortion embedding is the attractive feature of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be pleasing, particularly in military data and medical data. In such a circumstances, every small part of information is important. From the application point of view, since the differentiation between the implanted image and original image is almost discernible from human eyes, reversible data implanting could be thought as a top secret communication channel since reversible data implanting can be used as an information transporter.

3. LITERATURE SURVEY

A considerable amount of research on reversible data hiding has been done over the past few years. Some important techniques are discussed here. Various techniques have been proposed and research has been done in the field of reversible data hiding. Also many advanced methods have been introduced for reversible data hiding and visual cryptography. Some research work in the area of reversible data hiding is illustrated below:

Wei Liu et al. [4] 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. [5] 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.

Christophe Guyeux et al. [6] 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. [7] 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. [8] 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. [9] 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. [10] 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.

G. Boato et al. [11] 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. [12] 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. [13] 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 by inserting multiple watermarking.

HuipingGuo et al. [14] 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. [15] 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 the desired estimates but for security reason anti-collusion codes have yet to be employed.

4. CONCLUSION

With the increased use of internet, proposed system focuses mainly on RDH as the secured way of communicating over insecure channels of internet.

Reversible data hiding in encrypted images is a new topic getting attention because of the secured environmental requirements. Data hiding in reversible manner in encrypted images is providing double security for the data such as image encryption as well as data hiding in encrypted images both are done here.

The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner means, data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back. In future it may possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, DOI 10.1109/TCSVT.2015.2433194.

[2] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Information Forensics & Security*, 8(3), pp. 553-562, 2013.

[3] Shweta Patil Student, Electronics Amrutvahini college of engineering, Sangamner Maharashtra, India," Data Hiding Techniques: A Review" International Journal of Computer Applications (0975 – 8887) Volume 122 – No.17, July 2015.

[4] [4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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,

[14] 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–

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