International Research Journal of Computer Science (IRJCS)
Issue 09, Volume 4 (September 2017)
ISSN: 2393-9842
www.irjcs.com

RSA BASED IMAGE STEGANOGRAPHY USING REVERSIBLE DATA HIDING

G.S.Sowmiya[#1], Dr. K.Selva Bhuvaneswari[#2]
#1, Research Scholar, Department of Computer Science, University College of Engineering, Kanchipuram, INDIA
#2, Assistant Professor, Department of Computer Science, University College of Engineering Kanchipuram, INDIA

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue09/SISPCS10099**
Received: 08, September 2017
Final Correction: 13, September 2017
Final Accepted: 20, September 2017
Published: September 2017
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract-- Reversible data hiding is the methodology of inserting information bits by modifying the original image, but enables the exact lossless restoration of the original and the embedded information. This research focuses on the proposal of reversible image transformation (RIT) that enables efficient reversible data hiding (RDH). RIT based framework allows the user to transform the content of original image that looks like a targeted image and it can be used as "encrypted image" by any RDH methods. This is normally accomplished by Block pairing and Block transformation .This work additionally makes use of a process of semantic lossless compression technique that saves space for embedding extra data. Semantic compression implies that the compressed image is closer to the original image and gives a marked image with good visual quality. For reversible data hiding, an enhanced version of traditional RDH scheme is proposed. In RDH scheme, the marked image is used to reconstruct the image, Later the reconstructed image is used to extract the message. The proposed work is used to embed watermark in the encrypted image, which can satisfy different needs on image quality and large embedding capacity respectively. The quality of the encrypted image can be evaluated by various parameters such as MSE and PSNR.The space complexity of the proposed work can also be assessed for evaluating the performance.

Keywords: Reversible Data Hiding in Encrypted Image (RDH-EI), Reversible Image Transformation, Cryptography, Image Encryption.

I. INTRODUCTION

Cryptography technique is used to reformat and transform desired data, and making it safer on its trip between computers. This technology is purely depends on the essentials of secret codes, and then enlarged by modern mathematics that protects the data in powerful manner. Generally, it is about constructing and analyze protocols that block these third parties with the help of various aspects in information security such as data integrity, data confidentiality, authentication, and non-repudiation. Modern cryptography exists at the intersection of the rules and regulations of mathematics, computer science, image processing etc. cryptography provides several applications such as computer passwords, e-commerce etc. Although Cryptographic system generally classified by three independent dimensions. Steganography is a technique to hiding the information and an effort to conceal existence of the embedded data. Generally a plaintext message hidden by two ways. The methods of steganography hide existence of the message, whereas the method of cryptography renders the message incomprehensible to outsiders by various transformations of the text. Some researches states that it is a better way for securing message than cryptography technique and conceals the message content not the existence message. Here the original message is being hidden within a carrier such as the changes occur in the carrier but those are not visible.

Furthermore Steganography is a great tool allows to coverts transmission of data over on communications channel. Also capable to combine the secret image and carrier images that provide hidden image. But the hidden images are hard to detect without retrieval. Recently, Outsourcing photos to database and sharing photos through social media became a famous technology, at the same time protection is a challenging task. Traditional data hiding method appropriate for embed a small message into a large cover page, small test message or images. However, Reversible data hiding is an image hiding technique also it recovers the original cover without losses and recover the extracted message from embedded process; for example: labels, image metadata, notations or authentication information into the encrypted images. Generally the original image requires perfect recovery and hidden message from receiver side. Thus the technique preferred several applications such as law enforcement, Medical application; for example maintain the patient's information in secret manner, invisibility of secret hidden data military application where the invisibility of secret hidden data with high demands [2]. Also, this application requires lossless recovery of original image and hence requires reversibility. This paper proposes framework of Camouflage of Image by Reversible Image Transformation (RIT). RIT-based RDH-EI shifts semantic of original image to semantic of another image. Thus protects the privacy of original image and reversibility means that can be loselessly restored from converted image. Therefore RIT scheme viewed as a special encryption scheme, since the camouflage image in a form of plaintext, it will avoid the notation of the database server, and the database server can easily embedded extra data into the camouflage image with conventional RDH scheme for plaintext images.

II. LITERATURE REVIEW

Lee et al analyzed a transforming the secret image to a randomly selected target image without any use of database. In this method, each block of the secret image is transformed to a block of the target image with a reversible color transformation, and then required information for restoring secret image, namely indexes of block, parameters, added into the transformed blocks, which is used to proved that the Encrypted images. In this method, can transform a secret image to a randomly selected target image, and enhances the quality of encrypted image. However, authors stated that the transformation is not reversible, so that secret image cannot be losslessly reconstructed [3].

Celik et al. proposed a data hiding technique to quantize each image pixel using L-level scalar method. Residues yielded after quantization compressed using a lossless compression algorithm known as CALIC. Compacted residues beside with the to-be embedded bits are embedding into the quantized image using LSB alternate. Distortions introduced on the watermarked image by presented technique and it is comparatively higher [4].

Hong et al. introduced a novel method in decryption side by further making use of the spatial correlation using a different opinion equation and side match scheme to gain much lower error rate. Both methods obtained above rely on spatial correlation of original image to extract data. From this method image encrypted and decrypted before the data extraction [5].

Zhang et al. recovered the recursive code expansion for binary covers and effectively proved that the development gain the rate-distortion bound as long as the compacting algorithm reaches entropy, it launches the correspondence among the data compression and RDH for binary covers [6].

P Devaki et.al introduced a technique to achieve more efficiency in confidentially shares secret images or text and also authenticate the dealers. In this algorithm are combining the concepts of threshold secret sharing and image fusion [7].

Xinpeng Zhang planned a novel scheme for separable reversible data hiding in encrypted image. In a method, data owner encrypt the original un-compressed image with a encryption key and data hider condense least significant bits of encrypted image to create a sparse space to contain some supplementary data by using data hiding [8].

Lai et al. [9] presented a new image transformation technique to selects a target image similar to the secret image, then replaces each block of target image by a similar block of secret image and embeds the map among secret blocks and target blocks; it form an Encrypted image of the secret image. A greedy search method used to justify the most similar block. Although Lai et al.'s method is reversible, it is only suitable for a target image similar with the secret image, and the visual quality of encrypted image is not so good.

III. PROPOSED METHOD

This section describes a novel reversible image transformation technique, but this technique is not only improves quality of the encrypted image but also it can restore the secret image in lossless manner. Furthermore, it can share the data to the database. Therefore, the database can easily add additional data into the encrypted image by any RDH methods. It is very crucial to secure data and allows database server to manage data at the meantime. Under such demands, proposes a method of Reversible Data Hiding in Encrypted Image based on Reversible Image Transformation. Other from all existing encryption methods, RIT based method allow user to transmute data of original image into another target image with the same size.

Also it has secures original image, transmuted images appears like the target image which is used as the encrypted image, and the transmutation done among the micro blocks with small size, that improves the quality of the encrypted image.

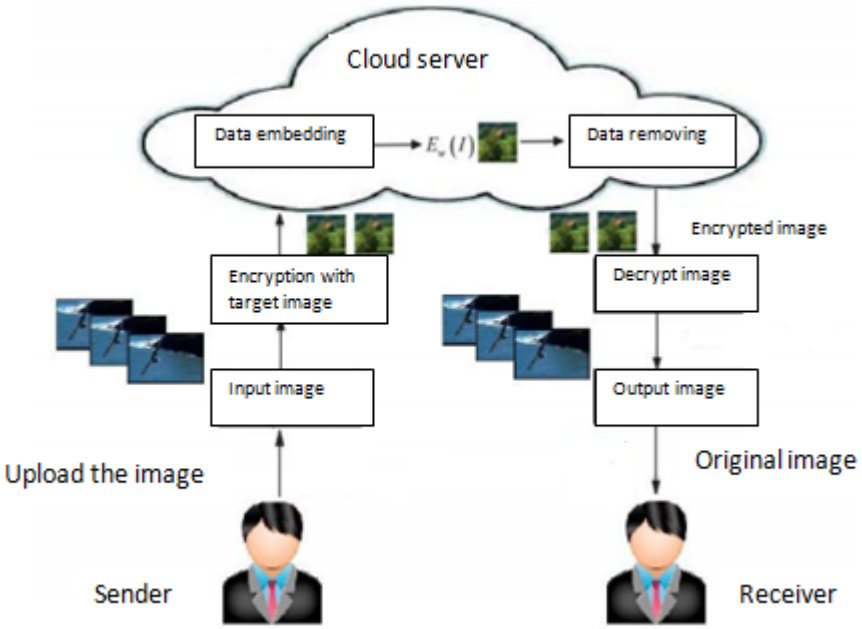

Fig: 1. Proposed block diagram

Reversible Image Transformation

A Secure Reversible Data Hiding Image Transformation using cloud storage where a user required uploading an image on database server. Once the user uploading the image in to the database at a time, user can choose a target image where the image can be embedded. The target image size must be greater than the input image size when a user uploads the image. After getting the image, it embedded into desire image and which is selected by the user. LSB based embedding techniques used for embedding data to the desired image. This image encrypted by using RSA encryption algorithm.

Generally, RSA algorithm is preferred for text encryption. As there is an important need for provide security on image transmission. In this work RSA algorithm is extended to perform image encryption and decryption. Initially, there are two prime integers's' and't' are taken which are used for scheming keys (private and public key) and selecting the input image for encrypting. 'b' and'd' are selected in such a way that =1. The selected image is encrypted by using the formula. 'S' is the input image we are encrypting. 'b' - public key used for encrypting process. Φ(m) is the product of (s-1) and (t-1) such that gcd (b,Φ(m)) =1. For example: e and Φ(n) are coprime. C is the cipher-image produced after encryption process. Then decrypt the encrypted image using the formula C is a cipher image after it has been encrypted. 'd' is the private key used to decrypt cipher image. 'm' is a product of (s-1) &(t-1); furthermore the complete derivations given as follows,

RSA Algorithm for Encryption and Decryption

1. Read the input RGB color image, G
2. First choose the two distinct prime numbers s and t.
3. Calculate the value, m = st.
4. Compute φ(m) = φ(s)φ(t) = (s − 1)(t − 1) = m - (s+ t -1), where φ is Euler's totient function.
5. Choose an integer b such that 1 < b < φ(m) and gcd (b, φ(m)) = 1; i.e., b and φ(m) are co-prime. b is the released as the public key.
6. Determined as d ≡ b −1 (mod φ(m)); i.e., b is the modular multiplicative inverse of e (modulo φ(y)). Solve the d given d·b ≡ 1 (mod φ(y)).
7. Obtain the encrypted image, C = Sb mod φ(m).
8. C = C mod 256, as gray level values of an image lie in the range [0,255].
9. Recover decrypted image, S = Cd mod 256.
10. The original input (recovered) image, R = S mod φ(m)

An ID based authentication method is used for authenticating the user. In the registration phase the user register to the system by providing their details these details are stored in the database storage. At the authenticating phase it verifies the users.

When the encrypted images are send to the DATA STORAGE it embed some data to the encrypted image and make it as watermarked image, and these watermarked image is stored in the cloud storage. When a download request come from a user its checks authentication and then removes the additional data which is added to make the watermarked images. At receiver side get encrypted image and it execute decryption to obtain the original image. This proposed system reduces the computation overhead at embedding, Data Storage, encryptions are perform at user side.

Reversible Data Hiding

The quality of the image gets disturbed when the data is embedded into the image. So it is expected that after the data extraction the image quality should be maintained just like the original image. But the image which is obtained contains some distortions. With regards to distortion in image, Kalker and Williams established a rate-distortion copy for RDH, through which they showed the rate-distortion bounds of RDH for without memory covers and proposed a recursive code development which, however, does not move towards the bound. Another promising strategy for RDH is histogram shift (HS), in which the space is saved where data embedded by shifting bins of the gray values histogram. This process follows three data embedding steps.

Step 1. Draw the histogram.
Step 2. Peak point is acquiring from consideration.
Step 3. Whole image scanned row by row.

After completion of the above process image involved under scanning process again. Example: If the grayscale value is 154 encountered, then the embedded data sequence checked & obtained a marked image. Thus data extraction is completed in effective way. To acquire the original quality of a cover, then the process of histogram shift applied again. The original cover obtained back. Basically, data hiding is the process to hide the data into some covering media; hence two data were used, namely embedding data and covering media. But in most of the cases the covering media acquire indistinct after the data embedded and the covering media is not inverted back to its original form after data removed from it [10]. Data embedding in reversible way which is the data embedding with no misfortune inserts the data or payload into advanced picture in reversible way. After data embedding the nature of unique picture might be debased which is to be maintained a strategic distance from? The appealing property of data embedding in reversible way is reversibility that is after data extraction the first quality picture is reestablished back. Reversible data embedding shrouds some data in an advanced picture such that an endorsed gathering could disentangle the concealed data and furthermore reestablish the picture to its unique state,

- **Visual quality**
- **Complexity**
- **Data embedding capacity limit**

The data with no bending embedding is the alluring element of reversible data embedding. Data will absolutely change the first substance by embedding a few data into it. Indeed, even an extremely slight change in pixel esteems may not be satisfying, especially in military data and restorative data. In such conditions, each little piece of data is critical. From the application perspective, Since the separation between the embedded picture and unique picture is practically noticeable from human eyes, reversible data embedding could be thought as a best secret correspondence channel since reversible data embedding can be utilized as a data transporter.

IV. RESULTS AND DISSCUSION

Fig: 2 Original image

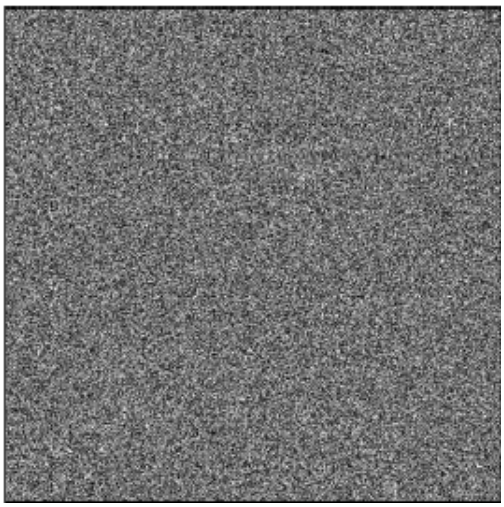

Fig 3: Encrypted image

Fig 4: Decrypted image

This section describes the result and discussion of the implementation. Figure: 2, 3 and 4 shows the original image, Encrypted image and Decrypted image respectively. Fig 5 and Fig 6 shows that the Average SSIM and PSNRs between encrypted images and marked images with different embedding payloads, comparing to the existing method the proposed method can achieve better results which shows that the efficiency.

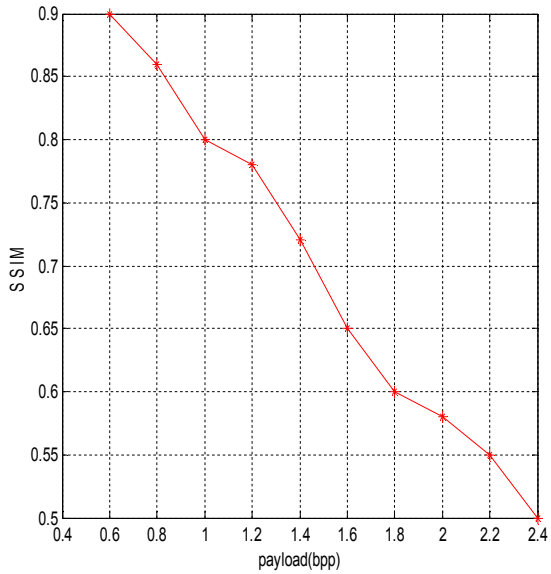

Fig 5: SSIM plot

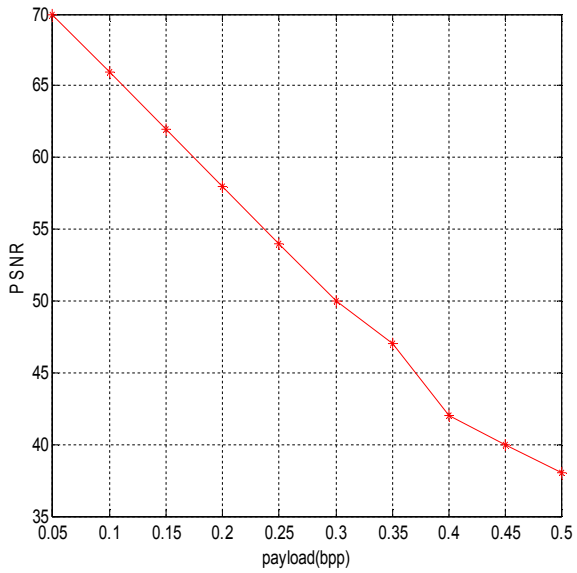

Fig 6: PSNR plot

V. CONCLUSION

Traditional reversible data hiding techniques have some limitations in encrypted image such as unable to protect image content, protect data privacy, low hiding capacity and multifaceted computations, poor clarity of the image, data compression etc and some problem in the decoding section. Under such demands, to overcome this kind of drawbacks the proposed novel framework transforms a secret image to a randomly selected desired image with good visual quality, and the secret image is restored without any loss. RSA algorithm is employed to modify image encryption. Image encryption and decryption approaches are highly securable and with less computational time it can protected the image content. So it is remarkable to implement RDH in encrypted images (RDH-EI), by which the data server can reversibly implant data into the image but cannot acquire any knowledge about the image contents.

REFERENCES

1. 2014Celebrity Photo Hack [online]: Available:http:/En.WIKIPEDIA.ORG/WIKI/2014_Celebrity_Ph oto_Hack.
2. F. Bao, R. H. Deng, B. C. Ooi, et al., "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. on Information Technology in Biomedicine, vol. 9, no. 4, pp. 554-563, Dec. 2005.

3. Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," IEEE Trans. Circuits Syst. & Image Technol., vol. 24, no. 4, pp. 695–703, 2014.
4. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding, in Proc. Int. Conf. Image Processing", vol. II, Sept. 2002, pp. 157160
5. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction, "IEEE Trans. Circuits Syst. Image Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
6. W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding(IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.
7. P Devaki and G Raghavendra Rao. "A novel algorithm to protect the secret image through image fusion and verifying the dealer and the secret image". In Signal and Image Processing (ICSIP), 2014 Fifth International Conference on, pages 77–80. IEEE, 2014.
8. Xinpeng Zhang. "Separable reversible data hiding in encrypted image". IEEE Transactions on Information Forensics and Security,7(2):826–832, 2012.
9. I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.
10. M.Johnson, P.Ishwar, V.M.Prabhakaran, D.Schonberg, and K.Ramchandran, "On com-pressing encrypted data," IEEE Trans. Signal Process, vol. 52, no. 10 Oct 2004., pp. 2992-3006.

