IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. VI (May-Jun. 2016), PP 32-36
www.iosrjournals.org

Hiding the Data into Meaningful Encrypted Image Using Reversible Data Hiding Technique

G.Malathi[1], Dr.S.Raju[2]
[1-]Student, [2-]Professor Department Of Computer Science And Engineering Sri Venkateswara College of Engineering Pennalur -602117

Abstract: *Data hacking is one of the challenging problems in Internet world. It is possible to greatly improve our understanding and also should provide security to network data. The most existing encryption algorithms designed to protect image contents transform original image into a texture-like or noise-like image which results in a significantly large number of attacks. A New Image Encryption System (NIES) concept is introduced to transform an original image into a visually meaningful encrypted one and to hide the data in image by using Reversible Data Hiding (RDH) technique. The proposed methods have potential applications for privacy and copyright protection in networks and cloud computing. In which gives effective protection to the secret data and also low computation cost.*

Keywords: *New Image Encryption System, Reversible Data Hiding.*

I. Introduction

Enormous amount of data emerges because of the modern social media. The data may be structured, semi structured and unstructured. The relational database has a predefined data model in which the structured data fitted into it. Mainly the structured data is based on the operational data (i.e., numeric, character, floating point, etc.) Semi structured data is a combination of structured and unstructured data. Semi structured data contain tags that separate the semantic elements and will not fit into formal data model. Unstructured data do not fit into relational data base and predefined data model. Unstructured data are text, audio, image, video and internet data. In this paper, unstructured data is used. These unstructured data occupies more storage like megabyte, gigabyte, terabytes, etc. There will be a problem to store these kinds of data.

In the computer society, cloud plays major role in past ten years. Cloud computing provides large amount of online spaces for storage in order to overcome the limitations of storage. The multimedia data has private, classified and value information, to protect this information from leakage, becomes major issues for individuals and organizations. Image Processing is a technique used to enhance raw images from various applications. To enhance images from spacecraft, space probes and military flights, many techniques are developed. Image Encryption is a tool used to protect multimedia data. Image Encryption algorithm has many technologies to protect images by changing the locations or their pixel values [3, 4]. These technologies contain two domain, frequency domain and spatial domain. Frequency image encryption can change the image data in frequency domain using coefficients like, discrete fractional Fourier transform, Quantum Fourier transform and Reciprocal-orthogonal parametric transform. Spatial image encryption algorithm contains two methods, Permutation and substitution [5, 6]. Permutation method will change the location of the pixel position, where the Substitution method will change the pixel values.

Both permutation and substitution method provides high level security to image content by encrypting the images into texture- like or noise -like encrypted images, such as Fig 1(a) and (b). However these kinds of images will indicates that they are encrypted and secret or valued information are encrypted in it [9]. In order to protect that, an original image is transformed into a meaningful encrypted image, by seeing it cannot be identified that they are encrypted Fig 1 (c). Nowadays data hacking is a major issue, in order to protect text data. For security reasons the text data can also be encrypted in that meaningful image. The text data can be encrypted using the reversible data hiding technique (RDH), which provides a lossless data retrieval.

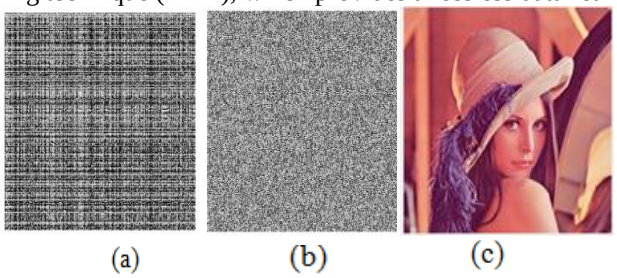


Figure 1-(a) Texture image **(b)** Noise image **(c)** Meaningful image

There are ways to implement this technique by using vacating room after encryption and reserving room before encryption [8]. Here first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Real reversibility is realized, that is, data extraction and image recovery are free of any error.

II. Related Works

'Reversibility improved lossless data hiding', was proposed by X.Gao, L.An, X.Li, D.Tao, (2009), recently, lossless data hiding has attracted increasing interests. As a reversible watermark scheme, the host media and hidden data should be recovered without distortion. A latest lossless data hiding technique based on image blocking and block classification has achieved good performance for image authentication. However, this method cannot always fully restore all the blocks of host images and watermarks. For this purpose, we propose an improved algorithm, which is characterized by two aspects [7].

First, a block skipping scheme (BSS) is developed for the host blocks selection to embed watermark; secondly, the embedding level is modified by a novel parameter model to guarantee that the host blocks can be recovered without distortion as well as the embedded data. Extensive experiments conducted on standard grayscale images, medical images, and color images have demonstrated the effectiveness of the improved lossless data hiding scheme. Consequently, in the proposed system not only recovers the host image and watermark without distortion, but also has the same merits as the previous one, i.e. (1) no salt-and-pepper noise, (2) capacity adjustment.

This framework, 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 lossless vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized 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.

Cryptography is a means of storing and transmitting data in a form that only targeted people can read or process. It is an effective way of protecting sensitive data stored on media or transmitted over unsecured network communication paths. On the receiving end, the encrypted information is then processed and decrypted by humans or machines to reveal the original message [1]. The goal of cryptography is to hide information from unauthorized individuals. The changes that cryptography has undergone closely follow advances in technology [2]. Image cryptography has many applications in various areas. Researchers may employ the traditional text cryptosystems to encrypt images directly; however, since image sizes are far greater than text, and differ in nature from normal text, traditional text encryption methods are not applicable to images. Image encryption methods can be classified into either lossy or lossless. In lossy encryption methods, were the image details are somewhat distorted, the resulting decrypted image is different from the original image. Due to the characteristics of human perception, and depending on the application, a decrypted image with little distortion is usually acceptable. However, lossless encryption methods are more applicable in applications where the distorted-free original image is required, such as in: medical images, aerospace images, satellite images, and in applications that involve highly classified images.

Iii. Proposed Work

In the existing system, New Image Encryption System (NIES) enhances the security with low computation cost using Discrete Wavelet transform (DWT) which transform original image into visually meaningful image and the reference image is larger than the original image. Original image is encrypted by any encryption algorithm. That encrypted image is stated as pre encrypted image. Then pre encrypted image is transformed by DWTCT algorithm, that is approximation, horizontal, diagonal, vertical. By adding a module that hides the text data into the encrypted image enhances the existing algorithm. The Reversible Data Hiding (RDH) technique is suitable to hide confidential data with high security.

Reversible data hiding technique which gives lossless data while decrypting the encrypted image. RDH also recover the image without any loss while encryption and decryption of image. It will reduce the computation cost and increase the protection over the contents.

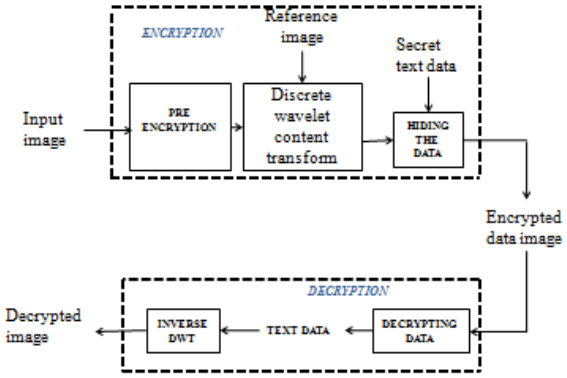


Figure 2 – Block Diagram of Proposed System

A. Pre Encryption Method:

In pre encryption method, the original image is processed to noise like or texture like image by using permutation and substitution methods. Where permutation method change the location of the pixel positions and substitution method will change the pixel value. Here Advanced Encryption Standards (AES) is used for encrypting the original image into pre encrypted image [12].

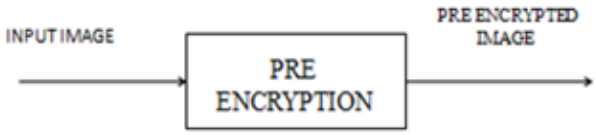


Figure 3 – Pre Encrypted Process

The pre encrypted image will be noise-like or texture-like image. Figure 3.1 shows the pre encrypted image.

Figure 3.1 – Pre encrypted image

B. Image Transformation:

In image transformation module, the pre encrypted image is transformed to vertical and diagonal part by using DWTCT and reference image is transformed into four sub bands and in vertical and diagonal part the original image value will be encrypted [10]. So pre encrypted image is transformed into visually meaningful encrypted image.

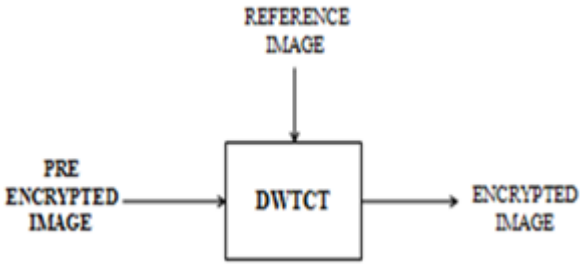


Figure 4 – Image Transformation process

Algorithm for dividing the pre encrypted image into vertical and diagonal. For example this pre encrypted image pixel value is 234, then 234/10 is equal to 23 and 234 mod 10 is equal to 4.

Input: Pre encrypted image X with a size of $m \times n$, reference image R with a size of $2m \times 2n$, and parameter Pt,

1: Apply DWT defined by parameter *Pt* to the reference image *Y*; obtain *CA*, *CH*, *CV* and *CD*
2: **for** *M*=1to*m* **do**
3: **for** *N*=1to*n***do**
4: *CV* (*M*, *N*) = *X* (*M*, *N*)/10
5: *CD* (*M*, *N*) = *X* (*M*, *N*) mod 10
6: **end for**
7: **end for**
8: Apply the inverse DWT to *CA*, *CH*, *CV* and *CD* sub bands
Output: The final encrypted image *E* with a size of 2*m*×2*n*.

Here *CA* is approximation, *CH* is horizontal, *CV* is vertical and *CD* is diagonal. Then the Pre encrypted image is splitted into two bands, that is, vertical and diagonal. Whereas the reference image will be transformed into four sub bands (Figure 4.1) .Where the first image is approximation , second image is horizontal , third image is vertical and four image is diagonal. So in this vertical and diagonal part the pre encrypted image values will be encoded. Then the original image is completely transformed into meaningful reference image.

Figure 4.1 – DWT image

C. Data Hiding:

In this method, hiding the data into encrypted image by using Reversible Data Hiding technique. The encrypted image is divided into two parts and in one part the secret text data will be added and encrypted into the encrypted image.

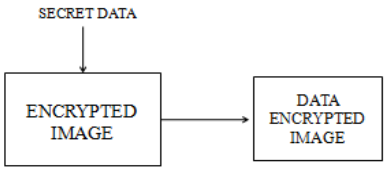


Figure 5 – Data Hiding Process

D. Decryption:

In this method, the encrypted image is decrypted by using inverse Discrete Wavelet Transform (DWT). The secret text data and original image is retrieved without any loss and error free data.

In image decryption, the encrypted image is firstly decomposed into four sub bands by the wavelet filters defined by *Pt*. There construction of the pre- encrypted image can be defined by,

$X(M,N)=10C'_V(M,N)+C'_D(M,N)$

Where C'_V and C'_D are sub bands corresponding to *CV* and *CD* of the encrypted image. *X* (*M*,*N*) is the reconstructed pre-encrypted image. So there will be no data loss during decryption process.

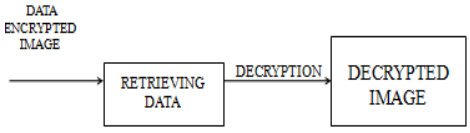
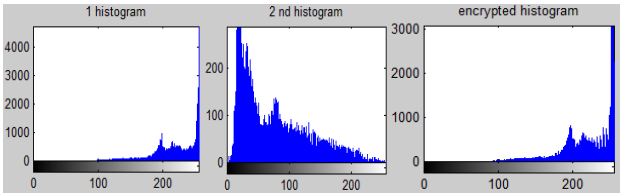


Figure 6 – Decryption Process

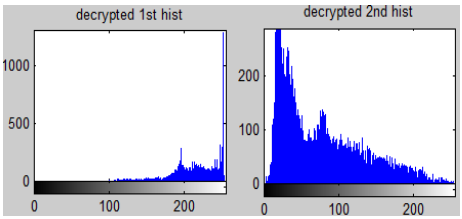
III. Result Analysis

For image encryption the original image and reference image has different histogram graph shown in (Figure 7.1). While decrypting the encrypted image, the same histogram graph value is received (Figure 7.2). So there will be no data loss and error in the proposed system.



(a) (b) (c)

Figure 7.1 – Encryption of two images (a) 1st image histogram (b) 2nd image histogram (c) Encrypted image histogram



(a) (b)

Figure 7.2 – Histogram of Decryption of encrypted image (a) decrypted 1st image (b) decrypted 2nd image

IV. Conclusion

The proposed concept is able to protect the original image with a much higher security level compared with most existing encryption algorithms. A new concept of image encryption is to encrypt meaningful encrypted images that usually are considered as normal images rather than encrypted ones. The proposed concept ensures the attackers' difficulty of correctly distinguishing and locating the encrypted images from all normal images.

An image encryption system utilizes a pre-encryption process to protect the original image contents, and an effective DWT based content transform to generate visually meaningful encrypted images with many different visual appearances and the proposed encryption concept and system show excellent encryption performance and enhance the security of existing image encryption algorithms with a low computation cost. The proposed methods have potential for security, lossless data and error free. It provides a low computation cost.

Reference

[1]. Y. Chen, Comment on ''Cheating prevention in visual cryptography'', IEEE Trans. Image Process. 21 (7) (2012) 3319–3323.
[2]. X. Zhang, Scalable coding of encrypted images, IEEE Trans. Image Process. 21 (6) (2012) 3108–3114.
[3]. M. Zanin, A. N. Pisarchik, Gray code permutation algorithm for high-dimensional data encryption, Information Sciences 270 (0) (2014) 288–297.
[4]. Y. Q. Zhang, X. Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, Information Sciences 273 (0) (2014) 329–351.
[5]. S. Tedmori, N. Al Najdawi, Image cryptographic algorithm based on the haar wavelet transform, Information Sciences 269 (0) (2014) 21–34.
[6]. Y. Zhou, L. Bao, C. L. Philip Chen, A new 1D chaotic system for image encryption, Signal Processing 97 (2014) 172–182.
[7]. X. Gao, L. An, X. Li, D. Tao, Reversibility improved lossless data hiding, Signal Process. 89 (10) (2009) 2053–2065.
[8]. K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inf. Forensics Secure. 8 (3) (2013) 553–562.
[9]. Long Bao, Yicong Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences 324 (2015) 197–207.
[10]. A. R. Calder bank, I. Daubechies, W. Sweldens, B. L. Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmonic Analysis. 5 (3) (1998) 332–369.
[11]. X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (2010) 2714–2722.
[12]. L. Bao, Y. Zhou, C. L. P. Chen, H. Liu, A new chaotic system for image encryption, in: Proceedings of the 2012 International Conference on System Science and Engineering (ICSSE), 2012, pp. 69–73.