LIGHT WEIGHT CRYPTOGRAPHY BASED DIGITAL IMAGES STEGNOGRAPHY

[1]PRANIT JEBA SAMUEL C
Assistant Professor ,Department of EEE
K.Ramakrishnan College of Technology, Trichirappalli, South India

[2] Dr.A.Rajkumar
Professor ,Department of EEE
K.Ramakrishnan College of Technology, Trichirappalli, South India

ABSTRACT— Steganography is an ability of concealing information inside the cover in such a way it looks like simple cover though it has concealed information. There are many techniques to carry out steganography on electronic media, most especially audio and image files. In this method, we proposed a high secure steganography scheme hiding the image and text into cover image with different combination of Discrete Wavelet Transform light lightweight cryptography algorithms (DWT). Experimental results and case study provided the stego-image with perceptual invisibility, high security and certain robustness. The aim of this project is to propose a high-capacity image steganography technique that uses pixel mapping method in integer wavelet domain with acceptable levels of imperceptibility and distortion in the cover lightweight cryptography algorithms image and high level of overall security. This solution is independent of the nature of the data to be hidden and produces a stego image with minimum degradation.

Keywords: Stegnography,Lightweight Cryptography, data hiding

1. INTRODUCTION

In computer science, information hiding is the principle of segregation of the *design decisions* in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change). Written another way, information hiding is the ability to prevent certain aspects of a class or software component from being accessible to its clients, using either programming language features (like private variables) or an explicit exporting policy. Information hiding serves as an effective criterion for dividing any piece of equipment, software or hardware, into modules of functionality. For instance a car is a complex piece of equipment. In order to make the design, manufacturing, and maintenance of a car reasonable, the complex piece of equipment is divided into modules with particular interfaces hiding design decisions[1]. By designing a car in this fashion, a car manufacturer can also offer various options while still having a vehicle which is economical to manufacture.

The amount of digital pictures has exaggerated speedily on the net. Image security becomes more and more vital for several applications, e.g., confidential transmission, video police investigation, military and medical applications for instance, the need of quick and secure designation is important within the medical world. Nowadays, the transmission of pictures may be a daily routine and it's necessary to search out an economical thanks to transmit them over networks[2]. To decrease the coordinated universal time, the info compression is critical. The protection of this multimedia system knowledge is through with cryptography or knowledge activity algorithms. Since few years, a haul is to undertake to mix compression, cryptography and knowledge activity during a single step. For instance, some solutions were projected in to mix image cryptography and compression.2 main teams of technologies are developed for this purpose. The primary one relies on content protection through cryptography. There are unit many strategies to code binary pictures or grey level pictures. The second cluster bases the

Recent reversible knowledge activity strategies are projected with high capability, however these strategies don't seem to be applicable on encrypted pictures.

2. EXISTING SYSTEM

For instance, when the secret data to be transmitted are encrypted, a channel issuer without any know-how of the cryptographic key may also have a tendency to compress the encrypted records due to the constrained channel resource, a lossless compression method for encrypted gray image using progressive decompose and rate-well matched rapid codes is developed . With loss compression technique presented, an encrypted gray picture may be efficiently compressed by way of discarding the excessively rough and first-rate information of coefficients generated from orthogonal transform[4]. When having the compressed facts, a receiver may also reconstruct the primary content of unique image by means of retrieving the values of coefficients[6][7]. The computation of transform in the encrypted domain has also been studied. Based at the homographic houses of the underlying cryptosystem, the discrete Fourier transform within the encrypted area can be implemented.

A composite sign representation approach packing together some of sign samples and processing them as a completely unique sample is used to reduce the complexity of computation and the scale of encrypted statistics. There are also some of works on information hiding within the encrypted domain. In a purchaser–dealer water marking protocol, the vendor of digital multimedia product encrypts the authentic facts using a public key, after which permutes and embeds an encrypted fingerprint furnished by using the purchaser within the encrypted area[8]. After decryption with a private key, the consumer can achieve a watermarked product. This protocol ensures that the vendor cannot recognize the customer'swatermarkedversion whilst the customer can't recognize the authe ntic version.

3. PROPOSED SYSTEM

Modules Description:

3.1. Image Selection:

In this module choose the image that's cowl image to cover the information. Thus initial check the image that is valid to cover the information. We have a tendency to apply the bar chart check to examine the image with recognizable patterns[5]. A bar chart could be a graphical illustration of the distribution of knowledge. it's associate estimate of the likelihood distribution of an eternal variable. A bar chart could be a illustration of tabulated frequencies, shown as adjacent rectangles, erected over distinct intervals (bins), with a vicinity adequate to the frequency of the observations within the interval. the peak of a parallelogram is additionally adequate to thefrequency density of the interval, i.e., the frequency divided by the breadth of the interval. the whole space of the bar chart is adequate to the amount of knowledge. A bar chart might also be normalized displaying relative frequencies. It then shows the proportion of cases that comprise every of many classes, with the whole space equaling one. The classes area unit typically nominal as consecutive, non-overlapping intervals of a variable. In a a lot of general mathematical sense, a bar chart could be a operate mi that counts the amount of observations that comprise every of the disjoint classes (known as bins), whereas the graph of a bar chart is just a method to represent a bar chart. Thus, if we have a tendency to let n be the whole range of observations and k be the whole range of bins, the bar chart mi meets the subsequent conditions

$$n = \sum_{i=1}^{k} mi$$

3.1.1. Cumulative histogram

A cumulative histogram is a mapping that counts the cumulative number of observations in all of the boxes up to the specified bin. That is, the cumulative histogram Mi of a histogram mi is described as:

$$Mi = \sum_{j=1}^{i} (m_j)$$

3.1.2. Data hiding:

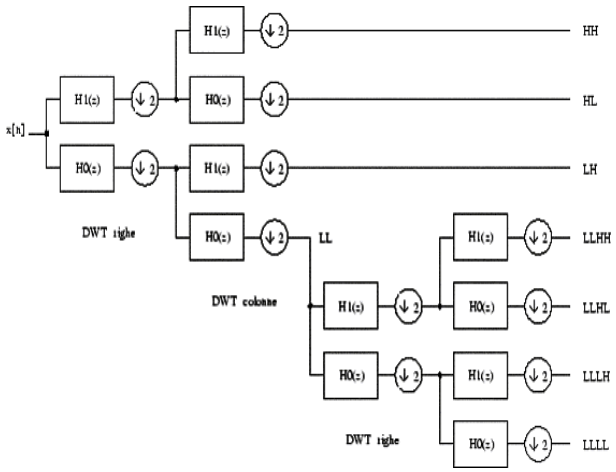
This module, we hide the statistics and choose the vicinity by means of the usage of DWT remodel. The information can be text or image. A discrete wavelet rework (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with different wavelet transforms, a key benefit it has over Fourier transforms is temporal resolution: it captures both frequency and region information. The DWT of a signal is calculated by way of passing it through a series of filters[11]. First the samples are passed thru a low skip filter out with impulse response resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k]$$

cc

$$ylow[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k]$$

$$yhigh[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k]$$



3.1.3. Encryption lightweight cryptography algorithm :

In this module encrypt the data by the usage of RSA set of rules. RSA entails a public key and a personal key. The public key may be recognized by everybody and is used for encrypting messages. Messages encrypted with the general public key can best be decrypted in a reasonable amount of time the usageof the personal key.

3.1.4. KeyGeneration:

Choose two distinct high numbers p and q
Compute n = pq.
Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1)
Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1; i.e. E and φ(n) are co-prime.
Determine d as D−1 ≡ e (mod φ(n)), i.e., d is the multiplicative inverse of e (modulo φ(n))[16][17].

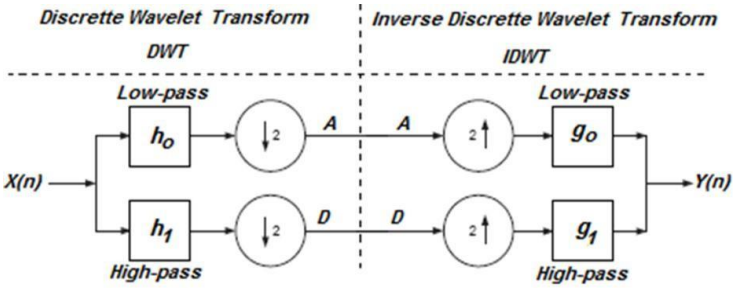
3.1.5. RSAEncryption:

M into an integer m, such that 0 ≤ m < n by the usage of an agreed-upon reversible protocol referred to as a padding scheme. He then computes the cipher textual content c corresponding to

3.1.6. RSADecryption:

Perform the decryption algorithm to extract the statistics from stenographic image.

3.1.7. Dataextraction:



Perform inverse DWT approach to extract picture and extract the records. Given the coefficient collection s(M) for some M

$$Sn^{(k+1)} = \sum_{k=-N}^{N} a_k S^{(k)}_{(2n-k)} + \sum_{k=-N}^{N} b_k d^{(k)}_{(2n-k)}$$

(or)

$$Sn^{(k+1)}(z) = a(z).(\uparrow 2)\left(s^{(k)}(z)\right) + b(z).(\uparrow 2)\left(d^{(k)}(z)\right)$$

For *k=J-1, J-2,...,M* and all n∈ z. In the Z-transform notation:

The up sampling operator $(\uparrow 2)A$creates zero-filled holes inside a given sequence. That is, every second element of the resulting sequence is an element of the given sequence, every other second element is zero or

$$(\uparrow 2)(C(z)) = \sum_{n\in z} C_n Z^{(-2n)}$$

This linear operator is, in the Hilbert space $l^2(Z, R)$ the adjoin to the down sampling operator.$(\downarrow 2)$

4. RESULT OF THE EXPERIMENT

The projected info concealing set of tips has been finished to several distinct kinds of pictures, like some generally used pix, clinical footage, texture footage, aerial pix, and every one the many photos inside the Corel DRAW info, and has perpetually achieved first-rate results, for this reason demonstrating its trendy pertinence. The projected facts concealing approach is in a position to imbed concerning 5–80

K into a photograph at the equal time as making sure the PSNR of the marked image versus the precise image. Additionally, this algorithmic program is also distributed to definitely every kind of pictures. In fact, it's been properly enforced to several of times used pix, clinical pix, texture images, aerial photos, moreover, this set of rules is pretty easy, and therefore the execution time is as an alternative short. Therefore, its basic standard overall performance is best than several contemporary reversible statistics concealing algorithms. it's anticipated that this reversible statistics concealing technique is also deployed for a good form of applications within the regions like steady scientific image info systems, and image authentication within the medical space and enforcement, and therefore the opposite fields within which the rendering of the actual photos is needed or desired. The fee distortion curves of the four snap shots Lena, Man, Lake and catarrhine. Here, three outstanding metrics are accustomed certificate the distortion in instantly decrypted photo: PSNR, the Watson metric and a universal best index letter. Whereas PSNR undoubtedly indicates the strength of distortion elicited by facts concealing, the Watson metric is meant by the usage of traits of the human sensory system and measures the entire sensory activity error; this is often DCT-primarily primarily based and takes under consideration three factors: comparison sensitivity, brightness protective and analysis overlaying. To boot, the tremendous index letter works in spacial domain, as a mix of correlation loss, brightness distortion and analysis distortion. within the ones figures, at a similar time because the cartesian coordinate represents the embedding charge, the ordinate is that the values of PSNR, Watson metric or exceptional index letter. The curves square measure derived from distinctive L, M and S beneath a circumstance that the precise content is also absolutely recovered victimisation the records concealing and encoding keys. Since the spacial correlation is exploited for the content recovery, the rate-distortion overall performance in a very electric sander image is best. The final performance of the non-separable technique is additionally given in Figure. It should be visible that the final overall performance of the projected severable theme is considerably higher .Once meeting the simplest recovery condition, the projected theme has a median advantage of embedded records amount with equal PSNR rate in directly decrypted photograph, or a median advantage of PSNR price in like a shot decrypted photograph with same embedded statistics amount.

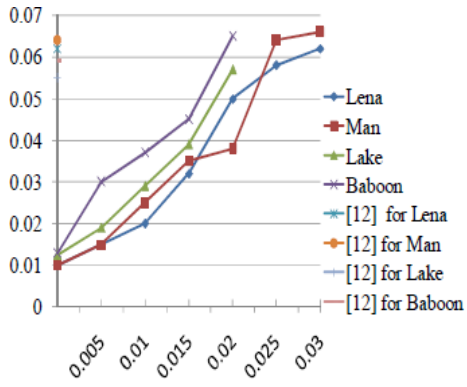


Fig.4.1. Performance Graph

Fig.4.2. Output Transmitted image

The rate distortion curves of the four pictures river, Man, Lake and Old World monkey. Here, 3 quality metrics were wont to live the distortion in directly decrypted image: PSNR, the Watson metric and a universal quality index letter of the alphabet. Whereas PSNR merely indicates the energy of distortion caused by knowledge concealing, the Watson metric is intended by mistreatment characteristics of the human sensory system and measures the entire sensory activity error, that is DCT-based and takes into consideration 3 factors: distinction sensitivity, light masking and distinction masking. To boot, the standard index letter of the alphabet works in spacial domain, as a mixture of correlation loss, light distortion and distinction distortion. Higher PSNR, lower Watson metric or higher letter of the alphabet suggests that higher quality. In these figures, whereas the Cartesian coordinate represents the embedding

rate, the ordinate is that the values of PSNR, Watson metric or quality index letter of the alphabet. The curves square measure derived from totally different L, M and S below a condition that the initial content are often dead recovered mistreatment the info concealing and cryptography keys. Since the spacial correlation is exploited for the content recovery, the rate-distortion performance in an exceedingly electric sander image is healthier. The performance of the non-separable technique is additionally given in Figure. It are often seen that the performance of the projected divisible theme is considerably higher. Once meeting the right recovery condition, the projected theme has a median gain of embedded knowledge quantity with same PSNR worth in directly decrypted image, or a median gain of PSNR worth in directly decrypted image with same embedded knowledge quantity.

5. CONCLUSIONS AND FUTURE WORK

Data hiding scheme for encrypted photo with a low computation complexity is proposed, which consists of picture encryption, information embedding and statistics extraction/ photo recuperation phases. The records of unique photograph are absolutely encrypted by a stream cipher. Although a records hider does not realize the original content, he can embed additional information into the encrypted photograph through modifying part of encrypted facts. With an encrypted image containing embedded records, a receiver can also firstly decrypt it the use of the encryption key and the decrypted version is much like the original photograph. According to the statistics hiding key, with the useful resource of spatial correlation in natural photograph, the embedded facts may be effectively extracted even as the authentic picture may be perfectly recovered. Although someone with the understanding of encryption key can achieve a decrypted photograph and hit upon the presence of hidden statistics using steganalytic methods, if he does now not realize the information hiding key, it is still impossible to extract the additional statistics and recover the authentic image. For making sure the correct facts extraction and the ideal photograph healing, it is able to permit the block aspect period be a large value or introduce error correction mechanism before information hiding to shield the additional facts with a value of payload reduction. The applied a reversible technique can be stronger in future by way of the use of the subsequent provisions and method can also be implemented after embedding when there is lot of change within the pixel to preserve nearest to the original price. It can be implemented in networking and the keys are dispatched and obtained securely. The image produced by using the reversible records hiding using key has distortion.

6. REFERENCES

[1] Bilgin A.et al., ―Scalable Image Coding Using Reversible Integer Wavelet Transforms,‖ Computer Journal of Image Processing IEEE Transactions, vol. 9, no. 4, pp. 1972 - 1977, 2000.
[2] Calderbank R.et al., ―Lossless Image Compression Using Integer to Integer Wavelet Transforms,‖ in Proceedings of International Conference on Image Processing, USA, pp. 596-599, 1997.
[3] Fridrich J et al ―Forensic Steganalysis: Determining the Stego Key in Spatial Domain Steganography,‖ in Proceeding of Electronic Imaging SPIE, Spain, pp. 631-642, 2005.

[4] Johnson N. and Jajodia S., ―Steganography: Seeing the Unseen,‖ IEEE Computer Magazine,vol. 25, no. 4, pp. 26-34, 1998.

[5] Lee K. and Chen H., ―A High Capacity Image Steganographic Model,‖ in IEEE Proceedings on Vision Image and Signal Processing, China, pp. 288-294, 2000.
[6] Lin T. and Delp J., ―A Review of Data Hiding in Digital Images,‖ in Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278, 1999.
[7] Lo Y et al, ―Wavelet Based Steganography and Watermarking,‖ Wavelets Reports, Cornell University, 1998

[8] Lu S.,‖ Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property‖ , Idea Group Publishing, 2005.
[9] Misiti M et al -Wavelet Toolbox for Use with MATLAB, User Guide MathWorks Inc., 2000.
[10] Naor M. and Reingold O., ―On the Construction of Pseudo Random Permutations,‖ Computer Journal of Cryptography, vol. 12, no. 1, pp. 29- 66, 1999.
[11] Popa R., ―An Analysis of Steganographic Techniques,‖ Working Report on Steganography, Faculty of Automatics and Computers, 1998.
[12] Provos N. and Honeyman P., ―Hide and Seek: An Introduction to Steganography,‖ Computer Journal of IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 32-40, 2003.
[13] Tolbal F., Ghonemy A., Taha A., and Khalifa S., ―Using Integer Wavelet Transforms in Colored Image Steganography,International Journal on Intelligent Cooperative Information Systems, vol. 4, no. 2, pp. 230-235, 2004.
[14] Walker S., A Premier of Wavelets and Their Scientific Applications, CRC Press, 1999.
[15] Westfeld A. and Bohme R., ―Exploiting Preserved Statistics for Steganalysis,‖ in Proceedings of 6th International Workshop on Information Hiding, Canada,
[16] Pranit Jeba Samuel C et al, ―Improved Lightweight Cryptography Algorithm using Machine Learning Approach on IoT Platform‖ , International Journal of Control and Automation, VOL.12 no.6,pp310 - 323,2019

[17] Pranit Jeba Samuel C et al , ―Stochastic Request Handling and Mutual Request Handling Scheme for Enhancing the performance and Security of NoC in Internet of Things Platform‖ , International Journal of Advanced Science and Technology, VOL.28 NO.15,PP512- 524,2019