Providing Network Security on Transferring of Digital Images using Encrypted Light Weight Cryptography

Pranit Jeba Samuel\(^1\), J. Heraa Joy\(^2\), M. Agalya\(^3\), A. Dhineshini\(^4\)
Department of Electronics and Communication Engineering
K. Ramakrishnan College of Technology, Trichy, Tamil Nadu, 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: Steganography, discrete wavelet transform, encrypted lightweight cryptography.

I. 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. 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. For instance, a car manufacturer may have a luxury version of the car as well as a standard version. The luxury version comes with a more powerful engine than the standard version. The engineers designing the two different car engines, one for the luxury version and one for the standard version, provide the same interface for both engines. Both engines fit into the engine bay of the car which is the same between both versions. Both engines fit the same transmission, the same engine mounts, and the same controls. The differences in the engines are that the more powerful luxury version has a larger displacement with a fuel injection system that is programmed to provide the fuel air mixture that the larger displacement engine requires. In addition to the more powerful engine, the luxury version may also offer other options such as a better radio with CD player, more comfortable seats, a better suspension system with wider tires, and different paint colors. With all of these changes, most of the car is the same between the standard version and the luxury version. The radio with CD player is a module which replaces the standard radio, also a module, in the luxury model. The more comfortable seats are installed into the same seat mounts as the standard types of seats. Whether the seats are leather or plastic, or offer lumbar support or not, doesn’t matter. The engineers design the car by dividing the task up into pieces of work which are assigned to teams. Each team then designs their component to a particular standard or interface which allows the sub-team flexibility in the design of the component while at the same time ensuring that all of the components will fit together. 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. 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 protection on knowledge activity, aimed toward on the Q.T. Nowadays, a brand new challenge consists to imbed knowledge in encrypted pictures. Previous work projected to imbed knowledge in an encrypted image by victimization an irreversible approach (of knowledge /of information) activity or data activity, aimed toward on the Q.T. A brand new plan is to use reversible knowledge activity algorithms on encrypted pictures by want to get rid of the embedded knowledge before the image secret writing. Recent reversible knowledge activity strategies are projected with high capability, however these strategies don’t seem to be applicable on encrypted pictures.

II. 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. When having the compressed facts, a receiver may also reconstruct the primary content of unique image by means of retrieving the values of coefficients. 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 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. After decryption with a private key, the consumer can achieve a watermarked product. This protocol ensures that the vendor cannot recognize the customer’s watermarked version whilst the customer can’t recognize the authentic version.

III. PROPOSED SYSTEM

I. Modules Description:

Image Selection:
In this module select the image that is cover image to hide the data. So First check the image which is valid to hide the data. We apply the histogram test to check the image with recognizable patterns. A histogram is a graphical representation of the distribution of data. It is an estimate of the probability distribution of a continuous variable. A histogram is a representation of tabulated frequencies, shown as adjacent rectangles, erected over discrete intervals (bins), with an area equal to the frequency of the observations in the interval. The height of a rectangle is also equal to the frequency density of the interval, i.e., the frequency divided by the width of the interval. The total area of the histogram is equal to the number of data. A histogram may also be normalized displaying relative frequencies. It then shows the proportion of cases that fall into each of several categories, with the total area equaling 1. The categories are usually specified as consecutive, non-overlapping intervals of a variable. In a more general mathematical sense, a histogram is a function $m_i$ that counts the number of observations that fall into each of the disjoint categories (known as bins), whereas the graph of a histogram is merely one way to represent a histogram. Thus, if we let $n$ be the total number of observations and $k$ be the total number of bins, the histogram $m_i$ meets the following conditions:

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

Cumulative histogram

A cumulative histogram is a mapping that counts the cumulative number of observations in all of the bins up to the specified bin.

That is, the cumulative histogram $M_i$ of a histogram $m_i$ is defined as:

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

Data hiding:

This module, we hide the data and select the place by using DWT transform. The data may be text or image. A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information.

The DWT of a signal $x$ is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response $g$ resulting in a convolution of the two:

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

The signal is also decomposed simultaneously using a high-pass filter $h$. The outputs giving the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass).
The filter outputs are then sub sampled by 2:

\[ y_{\text{low}}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n - k] \]
\[ y_{\text{high}}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n - k] \]

Encryption lightweight cryptography algorithm:

In this module encrypt the data by using RSA algorithm. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

Key Generation:

1. Choose two distinct prime numbers \( p \) and \( q \).
2. Compute \( n = pq \).
3. Compute \( \varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) \).
4. Choose an integer \( e \) such that \( 1 < e < \varphi(n) \) and \( \gcd(e, \varphi(n)) = 1 \); i.e. \( e \) and \( \varphi(n) \) are co-prime.
5. Determine \( d \) as \( d^{-1} \equiv e \pmod{\varphi(n)} \), i.e., \( d \) is the multiplicative inverse of \( e \) (modulo \( \varphi(n) \)).

RSA Encryption:

\( M \) into an integer \( m \), such that \( 0 \leq m < n \) by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text \( c \) corresponding to

\[ C \equiv m^e \pmod{n} \]

RSA Decryption:

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

\[ m \equiv c^d \pmod{n} \]

Data extraction:

Perform inverse DWT technique to extract image and extract the data. Given the coefficient sequence \( s^{(M)} \) for some \( M < J \) and all the difference sequences \( d^{(k)} \), \( k = M, ..., J-1 \), one computes recursively

\[ S^{(k+1)} = \sum_{k=-N}^{N} a_k s^{(k)}(2n-k) + \sum_{k=-N}^{N} b_k d^{(k)}(2n-k) \]

(or)

\[ S^{(k+1)}(z) = a(z) \cdot \left( \frac{1}{2} \right) \left( s^{(k)}(z) \right) + b(z) \cdot \left( \frac{1}{2} \right) \left( d^{(k)}(z) \right) \]

For \( k = J-1, J-2, ..., M \) and all \( n \in \mathbb{Z} \). In the \( Z \)-transform notation:

- The up sampling operator \( \left( \uparrow 2 \right) \) 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

\[ \left( \uparrow 2 \right) \left( C(z) \right) = \sum_{n \in \mathbb{Z}} c_n Z^{-2n} \]

- This linear operator is, in the Hilbert space \( l^2(\mathbb{Z}, \mathbb{R}) \) the adjoint to the down sampling operator \( \left( \downarrow 2 \right) \)

IV. RESULT OF THE EXPERIMENT

The proposed information hiding set of guidelines has been finished to many distinct styles of images, such as some typically used pix, clinical pictures, texture pictures, aerial pix, and all the several photos within the Corel DRAW database, and has constantly achieved first-rate results, for this reason demonstrating its modern applicability. The proposed facts hiding approach is able to embed about 5–80 kb into a photograph at the equal time as making certain the PSNR of the marked picture versus the specific picture. In addition, this algorithm may be carried out to certainly all kinds of images. In fact, it has been correctly implemented to many frequently used pix, clinical pix, texture photographs, aerial photos. Furthermore, this set of regulations is pretty simple, and the execution time is alternatively short. Therefore, its basic ordinary overall performance is better than many modern-day reversible statistics hiding algorithms. It is anticipated that this reversible statistics hiding technique may be deployed for a wide style of applications inside the regions such as steady scientific image information systems, and image authentication inside the medical area and law enforcement, and the opposite fields in which the rendering of the particular photos is wanted or desired.

The fee distortion curves of the 4 snapshot shots Lena, Man, Lake and Baboon. Here, 3 remarkable metrics have been used to diploma the distortion in straight away decrypted photo: PSNR, the Watson metric and a universal best index Q. While PSNR definitely indicates the strength of distortion induced by facts hiding, the Watson metric is designed by the usage of traits of the human visual system and measures the complete perceptual error; this is DCT-primarily based and takes into account 3
factors: comparison sensitivity, luminance protecting and evaluation overlaying. Additionally, the tremendous index Q works in spatial domain, as a mixture of correlation loss, luminance distortion and evaluation distortion. In the ones figures, at the same time as the abscissa represents the embedding charge, the ordinate is the values of PSNR, Watson metric or exceptional index Q. The curves are derived from unique L, M and S underneath a circumstance that the precise content may be perfectly recovered using the records hiding and encryption keys. Since the spatial correlation is exploited for the content recovery, the rate-distortion overall performance in a smoother image is better. The general performance of the non-separable method is also given in Figure. It may be visible that the general overall performance of the proposed separable scheme is significantly higher. When meeting the best recovery condition, the proposed scheme has an average advantage of embedded records quantity with equal PSNR rate in directly decrypted photograph, or an average advantage of PSNR cost in immediately decrypted photo with same embedded statistics quantity.

The rate distortion curves of the four images Lena, Man, Lake and Baboon. Here, three quality metrics were used to measure the distortion in directly decrypted image: PSNR, the Watson metric and a universal quality index Q. While PSNR simply indicates the energy of distortion caused by data hiding, the Watson metric is designed by using characteristics of the human visual system and measures the total perceptual error, which is DCT-based and takes into account three factors: contrast sensitivity, luminance masking and contrast masking. Additionally, the quality index Q works in spatial domain, as a combination of correlation loss, luminance distortion and contrast distortion. Higher PSNR, lower Watson metric or higher Q means better quality. In these figures, while the abscissa represents the embedding rate, the ordinate is the values of PSNR, Watson metric or quality index Q. The curves are derived from different L, M and S under a condition that the original content can be perfectly recovered using the data hiding and encryption keys. Since the spatial correlation is exploited for the content recovery, the rate-distortion performance in a smoother image is better. The performance of the non-separable method is also given in Figure. It can be seen that the performance of the proposed separable scheme is significantly better. When meeting the perfect recovery condition, the proposed scheme has an average gain of embedded data amount with same PSNR value in directly decrypted image, or an

V. 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.

VI. REFERENCES:


