ENHANCEMENT OF DATA SECURITY USING IMAGE STEGANOGRAPHY TECHNIQUE

V.SAI PRASANNA VENKATESH\textsuperscript{1}, V.S.GOKUL\textsuperscript{2}, Dr.R.RAMAN\textsuperscript{3}

\textsuperscript{1,2}Final Year Student, St.Joseph’s Institute Of Technology, Chennai, Tamil Nadu, India.

\textsuperscript{3}Assistant Professor, St.Joseph’s Institute Of Technology, Chennai, Tamil Nadu, India.

vspvenky7@gmail.com

Abstract: Data security is one of the most challenging problems in today's technological world. In order to secure the transmission of secret data over the internet, various methodologies have been presented over the last decade. The combined process of steganography and cryptography is used in recent times to develop a unique robust scheme. Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. There are many different carriers for steganography. Of which, most popular ones are digital images. Due to recent developments in steganalysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using steganalysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for covert communication between two private parties. The process involves the usage of Arnold transform to scramble the pixels of secret image which we are require to hide and send it in a cover image. The scrambled pixel data is then embedded into the cover image. The embedding process involves the usage of shape adaptive Discrete Wavelet Transform (SA-DWT) to decompose the cover image and then Qualified Significant Wavelet Trees (QSWTs) approach is incorporated in order to select the coefficients where the encrypted secret data is embedded.

Keywords: Data security, image steganography, cryptography, steganalysis, Discrete Wavelet Transform and Qualified Significant Wavelet Trees.

1. INTRODUCTION

In recent years with development of communication systems, the security of these systems have been increased, and many roles in a variety of communication systems have been proposed. Cryptography, Watermarking and Steganography are three ways to secure
digital data. In cryptography, digital data are encrypted with a key and it can be decrypted with the same key. This method cannot guarantee the security of data after decryption [1]. In the watermarking methods, the limited and specific information embedded into digital data to prevent unauthorized tampering [2]. Steganography is the art and skill of embedding a secret message inside the cover media that used for hide communication between two sides [3]. This method has been widely used in private and secure communication, and it is necessity in security applications [4]. Most type of digital data can be used as a cover media (such as picture, video, text and etc).

Steganography is an arrangement of concealed information’s through text, image, plaintext, images, and videos. But the image steganography is frequently used in the world of digital media. Steganography is literally means the covered graphy, which originated from Greek for communicating purpose and sharing the information. Initially the sharing of information was done using the wax tablet, invisible inks, microdots, digital signature and arranging of characters[5]. Depending upon the development of networks the hiding of information has statically improved using the proposed system of the above methods. Today the world is much more concern about their security and protection when they share the details about the information. Sometimes the information is stored in the digital computers and networks that are relevant to keep the topics so easily for communication[6]. People are conscious about their security, not to get revealed to the third person without the knowledge of the sender and intended receipts. One of the most significant methods of steganography is the image steganography since it has been playing a vital role in today’s computer and network imagination. Digital image steganography is frequently used for transmitting the details for communication process. Cryptography and steganography are most common terms for embedding the information. But whereas the cryptography have a bit of drawback than steganography because the encrypted message which was stored in a cover image is visible to the third person and using retrieval method the encrypted message is possible to be seen properly. The secret key is most prior password to open the hidden message so that the security becomes more eligible to contact into the carrier image. Sending the encrypted message will make the proposed system to indulge in terms of their security alignment[7].

There are three requirements for a good image steganography approach as shown in Fig. 1. But there exists a trade-off between these three requirements. If the capacity is increased, then imperceptibility is somehow compromised and vice versa. The transform domain methods in image steganography is immune to attacks like compression, filtering
etc., but they have limited capacity, offer high complexity and computational time. On the other hand, spatial domain offers high capacity and robustness and, they have less computational time and complexity[8].

![Image](image_url)

**Figure.1 Requirements of a good image steganography approach**

## 2. EXISTING WORK

There are two known methods for steganography. Spatial domain and Transform domain. In spatial domain method, the secret message bits are embedded directly in the cover media bits and usually they have simple algorithms [9]. LSB is one of the most well-known algorithms in this domain [10]. In this method, the secret message bits are embedded in cover media least significant bits. This changes are undetectable by the human eyes but they are detectable with statistical tests. In the LSB methods, the secure message size is small and the secure message bits destroy in any compression [11]. There are various techniques that can be used in spatial domain such as LSB technique, Pixel Value Difference (PVD) technique, Edge based, Random pixel selection, Pixel mapping method, Texture based, Histogram based, etc[8].

The transform domain based techniques include transformation of cover image using frequency domain or wavelet domain[12]. After transforming the cover image, the data is hidden in the transformed image and then it is retransformed. It thus provides a complex procedure to hide the data in the cover image making image manipulation harder. The transform domain methods that are mostly used are Discretecosine transform (DCT), Discrete Fourier transform (DFT), Wavelet transforms like Discrete wavelet transform (DWT), Integer wavelet transform (IWT), and Curvelet transform (DCVT).
3. PROPOSED WORK

In proposed work we use an extra level of security to the secret data which we send to the receiver side by ensuring the right user to retrieve and access it. We have also tried to increase the robustness and hiding capacity a level higher than the techniques which are already existing. Along with Discrete Wavelet Transform (DWT) which we use for two level decomposition of the image we also use the Qualified Significant Trees (QSWTs) estimation in order to find and select most significant sub-band pairs to embed the secret data in it. First step is to select secret image and encrypt using the Arnold Transform.

ARNOLD TRANSFORM:

Arnold transform is one of the image scrambling mechanism used as a method of encryption. The technology of the image scramble is to change a given digital image to a disorder one and let its true expression of information cannot be intuitive, even if the calculation of all possible combination of circumstances will take a high price. However, if we know the parameters used in the method of scrambling, we just use the inverse scrambling to restore the original image. Therefore, the scrambling can be used as a method of image encryption, and also as a means of further pre-processing image information hiding.

The transform is a process of clipping and splicing that realign the pixel matrix of digital image. A two dimension Arnold transform is shown as follows:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N
\]

Where \(x\) and \(y\) are the coordinates of the pixel; \(N\) is the height or width of the square image processed; \(x'\) and \(y'\) are the coordinate of the scrambled image. The transform changes the position of two pixels, and if it is done several times, a disordered image can be generated.

The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image. This paper presents a system that uses Arnold transform to encrypt an image. The number of times the transform is applied depends on a secret message expressed in a higher base. It is also called as the Arnold cat map and takes the logic from linear algebra and uses them to change the pixel position with respect to the original image.
Figure 2(a). A sample image showing the Linear view.

Figure 2(b). An Arnold map view

IMAGE EMBEDDING PROCESS:

The embedding process is consists of processing cover image by DWT and QSWTs. The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. The basic idea of the DWT for a two dimensional image is described as follows. An image is first decomposed into four parts of high, middle, and low frequencies (i.e., $LL_1$, $HL_1$, $LH_1$, $HH_1$ subbands) by critically subsampling horizontal and vertical channels using subband filters. The subbands labeled $HL_1$, $LH_1$, and $HH_1$ represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the subband $LL_1$ is further decomposed and critically subsampled. This process is repeated several times, which is determined by the application at hand. An example of an image being decompose into ten subbands for three levels is shown in Fig. 3.

Figure 3. Image decomposition using DWT
Each level has various bands information such as low–low, low–high, high–low, and high–high frequency bands. Furthermore, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). If \( I \) represents an image, the DWT and IDWT for can be similarly defined by implementing the DWT and IDWT on each dimension and separately. An original 512×512 Lena image and its DWT decomposition are shown in Fig. 4.

![Image of Lena image and its DWT decomposition](image.png)

**Figure 4. DWT using sample image**

**QUALIFIED SIGNIFICANT WAVELET TREE (QSWT):**

The proposed algorithm hides the encrypted information into the largest-value QSWTs of energy-efficient pairs of subbands. Compared to other related schemes, the incorporated approach has the following advantages:

- it is one of the most efficient algorithms of literature that facilitates robust hiding of visually recognizable patterns,
- it is hierarchical and has multiresolution characteristics,
- the embedded information is hard to detect by the human visual system (HVS), and
- it is among the best known techniques with regards to survival of hidden information after image compression.

Initially the extracted host object is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of subbands \((HL_2, HL_1), (LH_2, LH_1)\) and \((HH_2, HH_1)\). Afterwards, the pair of subbands with the highest energy content is detected and a QSWTs approach is incorporated in order to select the coefficients where the encrypted biometric
signal should be casted. Finally, the encrypted secret image is redundantly embedded to both subbands of the selected pair, using a non-linear energy adaptable insertion procedure.

**IMAGE EXTRACTION PROCESS:**

The stego image which consists of the encrypted secret is extracted at the receiver side by recovery process. First the image which we send cover checked whether the same image is present in the database of the receiver. At the receiver side we also include authentication to restrict the access of the data to the authorized person. The image which is sent as a cover image must be in the database of the user, then only the permission is granted to the user to access the file. The inverse of the above mentioned process is done at the receiver to retrieve the secret data by the authorised person. The reverse of the DWT called as the Inverse Discrete Wavelet Transform is performed to stego image. The required sub band pairs are formed and the secret image is separated. The decrypted secret image is then applied with the reverse Arnold Transform in order to perform the decryption. Then the user must provide password keys to access the secret image.

3. RESULTS AND PERFORMANCE EVALUATION

The proposed method produced a PSNR value of 85.67% which is pretty enough when compared to the existing methods. The images which we used as cover images and the stego image which consists of the embedded secret image looked almost same.

![Figure 5. Visual attack after embedding with proposed steganography (a) cover images (b) stego images.](image)

5. CONCLUSION

The focus of this paper is security and confidentiality of data. A new method of image steganography and cryptography is implemented in order to enhance the security and
also the data embedding capacity of the image. The proposed scheme falls into the category of spatial domain-based algorithms. Therefore, it suffers from the inherent shortcomings of these approaches, including resiliency against different attacks such as cropping and noising. The proposed algorithm can identify changes of data in transmission channel, but it doesn’t concern with reconstructing of the cropped or noised images. As the future work, we aim at designing a resistant algorithm against modification attack, which reconstruct modified images efficiently. The other important topic for our future work is to comparing the results of steganalysis attacks on our proposed method results with current literature.

REFERENCES


