DIGITAL IMAGE HIDING ALGORITHM FOR SECRET COMMUNICATION

T.Punithavalli[1], S. Indhumathi[2], V.Karthika[3], R.Nandhini[4]

[1]Assistant professor, P.A.College of Engineering and Technology, pollachi
[2]Student, P.A. College of Engineering and Technology, pollachi
[3]Student, P.A. College of Engineering and Technology, pollachi
[4]Student, P.A. College of Engineering and Technology, pollachi

Abstract

It is important to keep the image secret with the growing popularity of digital media's through world wide web to avoid geometric attacking and stealing of images. A new digital image hiding algorithm that provides the security of hidden image, Imperceptibility , Robustness, Anti attacking capability is proposed. To achieve this, two different algorithms are used in frequency domain. The first algorithm is Discrete wavelet transform(DWT) and the second one is Singular Value Decomposition(SVD). Wavelet coefficients of secret and carrier image is found using DWT. In this the images are divided into four frequency part called LL, LH, HL, HH. Low frequency component possess main information. So the low frequency part alone taken for the process of SVD to increase imperceptibility. The processed secret image is embedded into the transformed carrier image. From this implementation of new digital image hiding algorithm, image can be stored and transmitted without any loss in that image even after getting affected by external factors such as rotation and noise. The parameter used to test the robustness is peak signal to ratio (PSNR). The experimental results shows that the proposed method is more robust against different kinds of attacks.

Keywords: Image hiding, DWT, SVD, Frequency domain, Attacks.

--***--

1. INTRODUCTION

In recent years, the accessing of multimedia has become very easy because of the fast development of the internet. In other words, this development makes unauthorized, illegal access and manipulation of multimedia files over internet. Digital representation of signals brings many advantages when compared to analog representations, such as lossless recording and copying, convenient distribution over networks, easy editing and modification, durable, cheaper, easily reachable archival. Unfortunately, these advantages also present serious problems including illegal copying, modifying and pirating. Digital image hiding techniques provides a solution to overcome this problem. Digital image hiding is the process of hiding or embedding an imperceptible or secret image into the carrier image which contain perceptually irrelevant or redundant information can be used as covers for hiding images to prevent further misuse of an image. Image hiding is an important method to confuse the illegal destroyer so as to play a protection function. Further these techniques are also extended to carry vital information inside the carrier image for transmission and reception under privacy.

1.1 Requirements

Generally, a practical image hiding system embeds secret image into the carrier image to protect illegal copying, modifying and pirating of digital images and must meet requirements. Obviously, different applications have different requirements for image hiding system. Therefore, it

is quite difficult to have unique set of requirements that all image hiding systems must satisfy. The requirements with respect to high degree of security are as follows

i. Robustness : It refers to the ability of embedded image to be preserved even after distortions introduced by standard or malicious data processing, which may be either intentionally or unintentionally. These distortions are also known as attacks.

ii. Imperceptibility : The Imperceptibility of embedded image refers to its perceptual transparency. In other words, the human eye should not be able to detect differences between embedded image and cover image.

iii. Capacity : It refers to the maximum amount of information that can be hidden in the cover image. It directly affects the robustness and imperceptibility.

iv. Security : It refers to the fact that unauthorized persons should neither detect nor read the secret image. However it must be extracted correctly by the authorized user.

1.2 Techniques

According to the domain in which embedding is done, these techniques are divided into two categories:-

i. Spatial domain method
ii. Frequency domain method

Spatial domain is a straight forward method. LSB substitution is one of the example for spatial domain method, which modifies the lower order bit of carrier image to embed the secret image. It has the advantage of low complexity and easy implementation but problem with this method is low security, because it is possible to modify the secret image easily by setting all LSBs or pixels to zero.

Frequency domain method become popular for image hiding. These are more robust to image processing than spatial domain method. DFT, DCT, DWT are some algorithms belong to this category. In frequency domain secret image is embedded into transform coefficients of carrier image after applying any one of the frequency domain transform as compared to spatial domain image hiding methods , frequency domain image hiding methods are more complex and have high robustness against various attacks and good invisibility.

In recent years many image hiding schemes using these popular frequency domain transforms. In all frequency domain image hiding schemes, there is a conflict between robustness and invisibility.

2. PROBLEM STATEMENT

Several researchers have proposed many security algorithms to secure confidential information. Techniques used can be categorized into two subcategories. Firstly there are techniques that are based on encryption and cryptographic schemes. These techniques are used to secure information during the storage and communication. As a result the final data will be stored in encrypted format. The disadvantages of this technique is its large computational overhead. Therefore, now a days the encryption based methods are not used.

3. PROPOSED TECHNIQUE

3.1 Discrete Wavelet Transform

The DWT is nothing but a system of filters. There or two filters involved, one is the wavelet filter, and the other is the scaling filter. The wavelet filter is a high pass filter, while the scaling filter is a low pass filter. DWT performs single level decomposition and computes approximation coefficients matrix and details coefficients matrices based on wavelet decomposition filters specified. In digital image hiding method the most commonly used filters are Haar wavelet filter, Daubechies bi-orthogonal filters. Each filters decomposes the image into four sub bands called approximation sub band (LL), horizontal sub band (LH), vertical sub band (HL), diagonal sub band (HH). Approximation component contains the main or primary information and other component contains the secondary information. The main advantage of wavelet transform over Fourier transform is, the wavelets have additional property called time localization property.
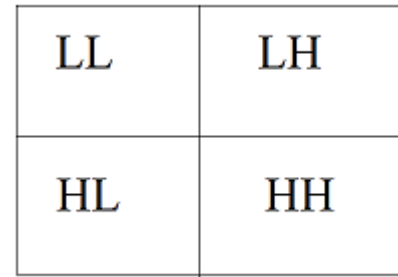

Fig.1 single level decomposition using DWT

3.2 Singular Value Decomposition

Singular value decomposition is a numerical method used to diagonalize matrix in numerical analysis. It is an algorithm developed for a various applications. Any matrix 'A' is decomposed into three sub matrices [u,s,v] such that: $A=u*s*v^T$. where 'u' and 'v' are the orthogonal matrices such that $u*u^T=I$ and $v*v^T=I$ where 'I' is the identity matrix and 's' is the diagonal matrix (s1,s2,s3……….sN) such that $s1>=s2>=s3…..s(N-1)>=sN$.

These values are known as singular values , and matrices u and v are known as corresponding singular vectors of matrix A. the above decomposition is called as singular value decomposition. A SVD, applied to the image, provides singular values or diagonal matrix 's' that represent the luminance or color intensity of the image while the matrices 'u' and 'v' represents the geometry of the image. It has been proved that slight variation in the singular values does not change the visibility of an image.

The main advantages of using this SVD is,
i. The singular values of an image has very good stability. Even when there is a little disturbance with A, it provides rotation invariance, translation invariance, transposition invariance, etc.
ii. SVD is used to represent the intrinsic algebraic properties of an image, where singular values corresponds to the brightness of the image and singular vectors corresponds to geometry characteristics of the image.
iii. An image matrix contains many small singular values compared with the first singular value. Even ignoring the small singular values in the reconstruction of the image does not affect the original quality of the reconstructed image.

These properties are much desirable in image hiding.

4.1 Embedding Process
i. Read the carrier image and resize it.
ii. Apply 1-level DWT on the carrier image. It provides four sub bands LL, LH, HL, HH. The LL sub band is taken for the embedding of secret image.

$$CA1 = CU + CS + CV$$

iii.   SVD is calculated for LL sub band only. This will reduce the computational complexity as we are not considering the whole carrier image.

iv.   Read the secret image and resize it as same as the carrier image.

v.   Apply DWT on the secret image

vi.   SVD is calculated for LL sub band of secret image.

$$SA1 = SU + SS + SV^{/}$$

vii.   Modify the singular values of LL sub band of carrier image.

$$E1 = CS + \alpha SS$$

Where, CS is the singular values of the carrier image and SS are the singular values of the secret image. α is the embedding strength.

$$CA1^{/} = CU + E1 + CV^{/}.$$

viii.   Perform the inverse DWT by combining the sub bands with the modified one to get the embedded image.
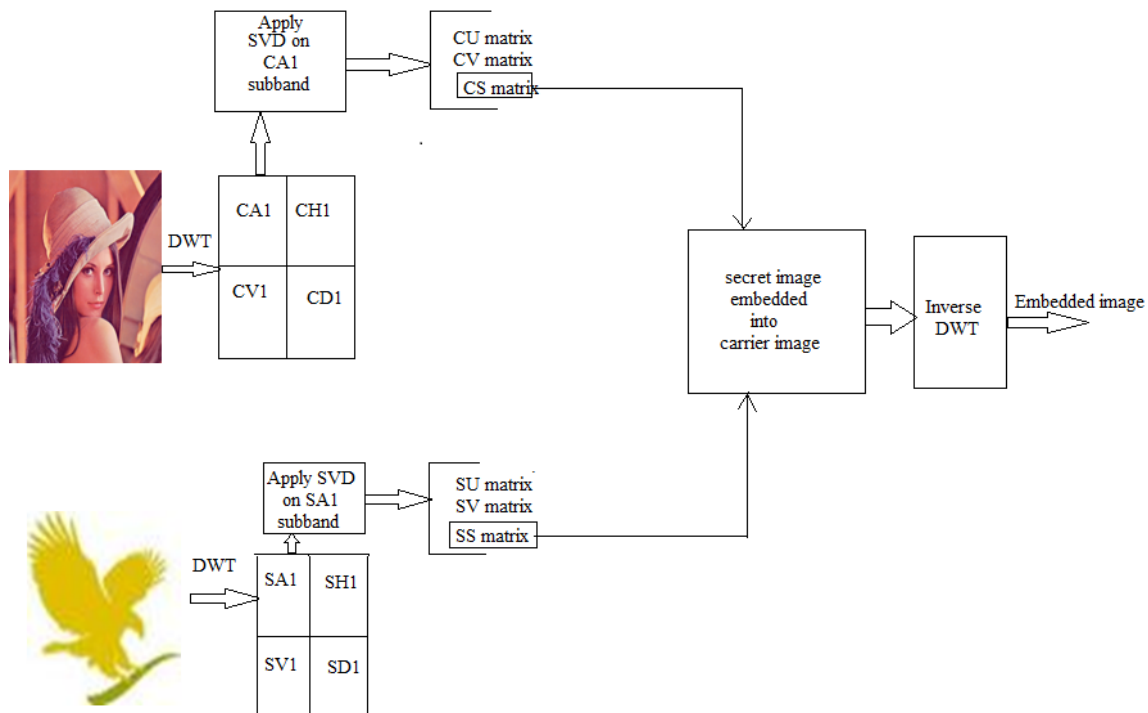

Fig. 2 Block diagram of embedding process

4.2 Extraction Process

The extraction technique is exactly the reverse of the embedding technique.

i.   Perform 1-level DWT on embedded image.

ii.   Perform SVD on the LL sub band.

iii.   Extract the singular values of the embedded image

$$SS_{extract} = (E1 - CS)/\alpha .$$

iv.   Perform IDWT by combining the all sub bands with the modified one to get the extracted image.
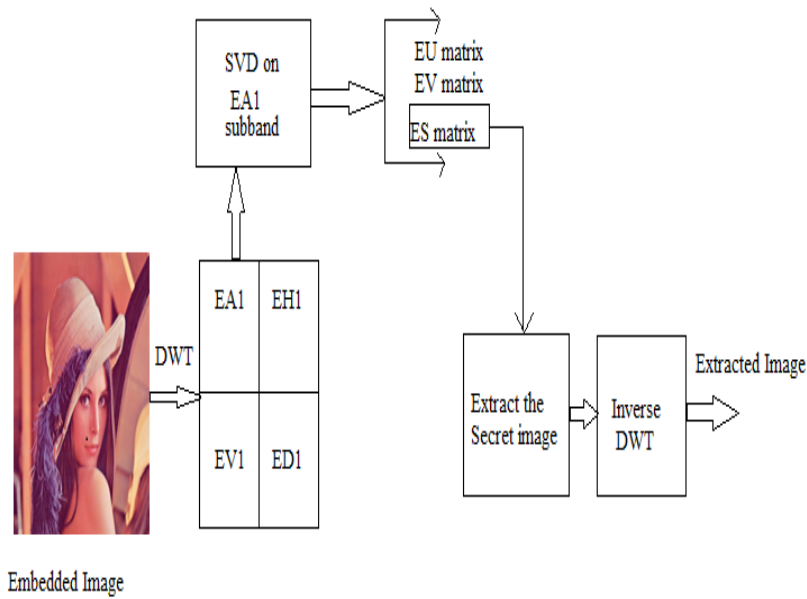
Fig 3. Block diagram of extraction process

5. ATTACK S

The attacks attempt to damage the embedded image by modifications of the whole image without any effort to identify and isolate the secret image. These attacks include frequency based compression, addition of noise, cropping and rotation.

Carrier Image

Secret Image

Embedded Image

Extracted Image

NOISE ATTACKS

Gaussian Noise (0.01)   Extracted Image

ROTATION

Embedded Image
Rotated by 90 degree

Extracted image

Rotated by -90 degree

Extracted image

Rotated by 180 degree   Extracted image

Fig 4. Extracted image after getting affected by various attacks

5.1 Analysis of PSNR Value

The proposed algorithm provides approximately constant PSNR value when attacks are introduced

ATTACKS	PSNR		
	R	G	B
No Attacks	35.3835	31.9404	32.3840
Gaussian Noise	34.2651	31.0819	31.2013
Rotation	33.1497	29.9462	30.3875

Fig 5. Table for comparison of PSNR values(with and without attacks)

6. CONCLUSION

In our simulation, we go through lot of test on image with size 512x512. One of them is in table1. Where we observe the PSNR value between original secret image and extracted secret image after applying attacks. The proposed algorithm improves the robustness and invisibility against various attacks except rotation (other than $90^{o},-90^{o},180^{o},-190^{o}$).

REFERENCES

[1]. Malashree K.S and Jagadish K.N, "Confidential Data Hiding Using Wavelet Based ECG Stenography", Journal of Engineering Research and Applications. Volume (4): issue(6), pp.84-88 may 2014.

[2]. Shuchi Sirmour and Archana Tiwari, "A Hybrid DWT-SVD based Digital Image Watermarking Algorithm for copyright Protection", International Journal of p2p Network Trends and Technology. Volume(6):ISSN 2249-2615,march (2014).

[3]. Honggin Shi, "DWT and SVD based Watermarking Scheme with Circulation", Journal of Software. Volume (9), Issue (3), March (2014).

[4]. Rathod Jigisha. D and Rachana Modi. V, "A Hybrid DWT-SVD for digital video watermarking", International Journal of Advanced Research in Computer and Communication Engineering. Volume (2), Issue (7),July(2013).

[5]. Naga Jyothi. T and Hari babu .T, "Non-Blind Watermarking Scheme for Image and Video Using DWT-SVD", International Journal of Engineering and Computer Science. Volume (2):Issue (11),ISSN:2319-7242,November(2013).

[6]. Pooja Malhotra and JyotiVerma, "A DWT-SVD based Watermarking Techniques for Digital Images", International Journal of Computational Engineering Research. Volume (3), Issue(6), June (2013).

[7]. Preeti Jain and Vijay Kumar Trivedi, "A Novel Technique for Data Hiding in Audio by Using DWTs", International Journal of Computational Engineering and Management. Volume (15):issue (4),pp.2230-7893,June(2012).

[8]. Samuel Manoharan .J and Sathesh."APerformance Analysis of Spatial and Frequency domain Multiple Data Embedding towards Geometric attacks", International journal of security. Volume (4):issue(3),2012.

[9]. Seema,"DWT-SVD Based efficient image Watermarking Algorithm to achieve high Robustness", International Journal of Advanced Research Computer Science and software Engineering. Volume (2), Issue (4), April (2012).

[10]. Yamben Jina Chanu and Manglem Singh. Kh, "Various Steganalytic Techniques Comparison for LSB Embedding", Trends in Innovative computing. Trends in innovative computing-information Retrieval and Data mining.2012.

[11]. Yu-Chen Hu, "High Capacity image hiding scheme based on vector quantization",Thejournal of The Pattern Recognition society.pp.1715-1724. February(2006).