International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Robust and Secure Steganography Scheme based on Singular Values Decomposition and Discrete Wavelet Transform

Y. S. Thakur[1], Brij Mohan Kumar[2]

[1]Professor, HOD, Electronics & Communication Eng. Dep't, Ujjain Engineering College, Ujjain

[2]PG Scholar, Digital Communication, Ujjain Engineering College, Ujjain

Abstract: ***Steganography is the study of embedding and hiding messages in a medium called a cover text. Steganography is related to cryptography . It was used by the Ancient Greeks to hide information about troop movements by tattooing the information on someone's head and then letting the person grow out their hair. Simply put, steganography is as old as dirt. The simple fact is that an encrypted message does not resemble anything else but an encrypted message. Once a third party determines that you are communicating in secret, they may feel compelled to force you or the person you are communicating with to tell them what you are hiding. The basic idea behind cryptography is that you can keep a message a secret by encoding it so that no one can read it. If a good cryptographic cipher is used, it is likely that no one, not even a government entity, will be able to read it. Two most important prerequisites for an efficient secret messaging scheme are robustness and security. Secret message must be robust and recoverable even if a part of content is altered by one or more attacks like compression, filtering, geometric distortions, resizing, etc. In this work, we propose a blind secret messaging scheme based on the discrete wavelet transform (DWT) and singular value decomposition (SVD). Singular values (SV's) of high frequency (HH) band are used to optimize perceptual transparency and robustness constraints. Although most of the SVD-based schemes prove to be robust, little attention has been paid to their security aspect. Therefore, we introduce a signature based authentication mechanism at the decoder to improve security. Resulting blind secret messaging scheme is secure and robust.***

Keywords: Authentication; security; secret messaging

1. Introduction

Fast development of digital technologies has improved the ways to access information. These new technologies enable us to store, transfer and process digital content with less time, lower complexities and better efficiency. However, digitization also brings in disadvantages like illegal reproduction and distribution of digital content. Internet plays a very crucial role in circulation of illegal and unauthorized digital content. This increases the risk of violating owner right and hampering authenticity of a digital content. One way to protect digital content against illegal reproduction and distribution is to embed some extra information into it. The information should be embedded in secure and robust manner such that it remains resistive to malicious attempts of removal [1]. Usually the information is about the digital content it intends to protect. A steganographic message should be embedded in such a way that it remains detectable as long as the perceptual quality of the digital content stays at an acceptable level [2].

2. Steganography: A Brief Introduction

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level[4]. Hiding information into a medium requires following elements [2]

1) The cover medium(C) that will hold the secret message.
2) The secret message (M) may be plain text, digital image file or any type of data.
3) The stegonographic techniques
4) A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types:

1) Text Steganography
2) Image Steganography
3) Audio Steganography
4) Video Steganography
5) Protocol Steganography

3. Previous Works

So far many steganographic schemes have been proposed with the intentions of improving robustness vis-a-vis perceptual quality. Compression is most common form of attacks in steganography. Two widely used image

compression standards are JPEG and JPEG2000. The former is based on the discrete cosine transform (DCT), and the latter is based on discrete wavelet transform (DWT). Many steganographic schemes which are robust against compression have been developed using these transforms. Raval & Rege (2003)[5] proposed a DWT based multiple steganographic schemes. Image was decomposed in two levels and secret messages were inserted in LL (low frequency) and HH (high frequency) bands. The scheme showed good results against wide range of attacks like compression, noise addition, histogram equalization but could not resist rotation, scaling and print-scan attacks. Kasmani & Naghsh-Nilchi (2008)[6] proposed a combination of DWT and DCT to embed the binary steganography. They performed 3-level DWT decomposition and then applied DCT to embed the secret message. Results showed a good message recovery against many attacks but this scheme suffers from high time complexity. Moreover, it had a non-blind detection. Recently singular value decomposition became very popular in steganographic schemes due to its attractive mathematical features. In the next part, we briefly discuss SVD and its role in the steganography.

3.1 Singular value decomposition (SVD)

SVD is one of the most useful tools in linear algebra with several applications in image compression, steganography, and other signal processing areas. If A is an nxn matrix, then SVD of matrix A can be defined as

$$A = U*S*VT, \quad (1)$$

Where U and V are the orthogonal matrices and S is a diagonal matrix. Diagonal elements of S are the singular values and they satisfy the following property

$$s(1,1) > s(2,2) > s(3,3) >.....> s(n, n). \quad (2)$$

SVD is popular for the secret messaging (Andrews & Patterson 1976; Zhou & Chen (2004)[7] because

1) Few singular values can represent large portion of signal energy,
2) SVD can be applied to square and rectangular images,
3) The SV's (singular values) of an image have very good noise immunity, i.e., SV's do not change significantly when a small perturbation is added to an image intensity values,
4) SV's represent intrinsic algebraic properties.

From table 1 we conclude that singular values are fairly robust against perturbation. Due to its robustness against noise, SVD became a popular tool in steganography domain.

Table 1: Variation in singular values after applying attacks

Image	S1	S2	S3	S4
Lena image (original values)	151.5234	42.2745	36.1516	27.9067
JPEG Compression (Q = 20)	151.6007	42.2129	36.0787	27.6894
Rotation (15°)	144.1636	48.0665	39.9409	28.7351
Scaling (512->256->512)	152.1418	42.1731	36.0141	27.7552
Scaling (512->1024->512)	152.7299	42.2633	36.1170	27.8758
Gaussian noise (M = 0, Var = 0.01)	158.5279	40.7767	35.4015	27.3755
Salt and pepper noise (M = 0, Var = 0.01)	152.3987	41.9533	35.8831	27.7077
Median filter [3×3]	151.2235	42.3403	36.1912	27.9125
Histogram equalization	151.5234	42.2745	36.1516	27.9067

3.2 Steganography Schemes based on SVD

In recent years several steganography algorithms have been proposed based on SVD. The main idea in these approaches is to compute the SVD of a cover image and then modify singular values to embed the message. Some algorithms used only SV's to embed the message. Recently hybrid steganography algorithms have been proposed where different transforms domain are used with SVD. In the following subsection, some of the popular SVD based schemes are discussed.

3.2.1 Pure SVD based schemes

Many of the earlier algorithms, based on SVD, embeds secret message directly into singular values. For example, Liu & Tan (2002) [8]proposed an algorithm in which secret message was embedded into the SVD domain and the detection was blind in nature. Results showed that scheme proved resilient against compression, filtering, cropping but could not resist rotation, scaling and print-scan attacks.

Ghazy et al (2007) [9] divided the image into non-overlapping blocks and then applied SVD to these blocks. Singular values of these blocks were used to embed the secret message. This scheme gave good results against compression, filtering, noise addition but failed against cropping and geometric attacks.

With an aim to increase the robustness of secret messaging scheme Bhandari et al (2005)[10] used spread spectrum (SS) along with SVD. They used two secret messages during embedding; one was inserted using spread spectrum technique and other by pure SVD. SS techniques provided robustness against compression, rotation, filtering, scaling, print and scan attack, while, SVD offered good robustness against noise addition and histogram equalization. Hence, these two complementary techniques covered wide range of attacks however, scheme was non-blind in nature.

3.2.2 Hybrid SVD based schemes

The SVD schemes which are using transform domain coefficients for decomposition are called hybrid SVD schemes. DCT, DWT, FFT are among popular frequency transforms. A hybrid method based on DCT and SVD has been proposed by Quan & Qingsong (2004) [11]. They applied DCT to the cover image and coefficients are mapped to frequency bands using zig-zag scanning. SVD was then applied to each band. Singular values of the DCT-transformed visual secret message are then used to modify the singular values of each band of the cover image. Results displays robustness against compression, filtering and cropping but secret message cannot survive against geometrical attacks and print-scan attack. The scheme was computationally expensive and non-blind in nature. A SVD based algorithm using DWT has been presented by Ganic & Ahmet Eskicioglu (2004)[12] which is very similar to the algorithm by Quan & Qingsong (2004)[13]. The cover image is decomposed using DWT into four sub bands. SVD is applied to each sub band and also to the secret message. Singular values of the cover image are modified using the singular values of the secret message during embedding process. This scheme gives comparatively good results vis-

a-vis all the schemes discussed so far. Study in this section shows that robustness of SVD-based secret messaging schemes is reasonably good but it can be improved using suitable combination of the transform domain and SVD.

4. Proposed Scheme of Secret Messageing

We propose a basic secret messaging which is based on cascading DWT with SVD. DWT decomposes the image into four frequency bands: LL, HL, LH, and HH band. LL band represents low frequency, HL and LH represent middle frequency and HH represents high frequency band, respectively. LL band represents approximate details, HL band gives horizontal details, LH provides vertical details and HH band highlights diagonal details of the image. In this proposal, we select HH band to embed the secret message because it contains the finer details and contributes insignificantly to the image energy. Hence secret message embedding will not affect the perceptual fidelity of cover image. Moreover, high energy LL band coefficient cannot be tweaked beyond certain point as it will severely impact perceptual quality. Also, Raval & Rege (2003) observed that secret message inserted in HH band survives certain image processing operations like noise addition, intensity manipulation and limitation of the human visual system can be exploited by inserting secret message into HH band. HVS fails to differentiate changes made to HH band.

The proposed scheme is based on the idea of replacing singular values of the HH band with the singular values of the secret message. In table 2, singular values of the HH band of different test images are given. It is observed that singular values lie between 84 and 173. If a secret message is selected such that its singular values lies within the given range, then the energy of the singular values of secret message will be approximately equal to the energy of the singular values of the HH band. Hence the replacement of the singular values will not affect perceptual quality of image and the energy content of HH band.

Table 2: Singular values of HH frequency band of different test images

Image	Singular values	
	Max	Min
Lena	142.6490	0
Bubble	84.7352	0
Building	173.2125	0
Cameraman	109.2292	0

Secret message used for experimentation in this scheme is preprocessed to have singular values within the range of 0–150 and it closely matches the singular values of the given test images. Secret message size is made equal to the size of the HH band.

4.1 Secret message embedding algorithm

(i) Secret message W is decomposed using SVD

$$W = Uw * Sw * VwT. \quad (3)$$

(ii) Apply Haar wavelet and decompose cover image into four sub-bands: LL, HL, LH, and HH.

(iii) Apply SVD to HH band.

$$H = UH * SH * VH T. \quad (4)$$

(iv) Replace the singular values of the HH band with the singular values of the secret message.

(v) Apply inverse SVD to obtain the modified HH band.

$$H' = UH * Sw * VH T. \quad (5)$$

(vi) Apply inverse DWT to produce the secret messaged cover image.

4.2 Secret message extraction algorithm

(i) Using Haar wavelet, decompose the noisy secret messaged image into four sub-bands: LL, HL, LH, and HH.

(ii) Apply SVD to HH band.

$$H = UH * SH * VH T. \quad (6)$$

(iii) Extract the singular values from HH band.

(iv) Construct the secret message using singular values and orthogonal matrices Uw and Vw obtained using SVD of original secret message.

$$WE = Uw * SH * VwT. \quad (7)$$

This constitutes a blind decoding as secret message extraction process does not require original cover image for extracting the secret message at the receiver. The above steps has been implemented and shown below:

1. First the program asks the user to select the cover image as shown below

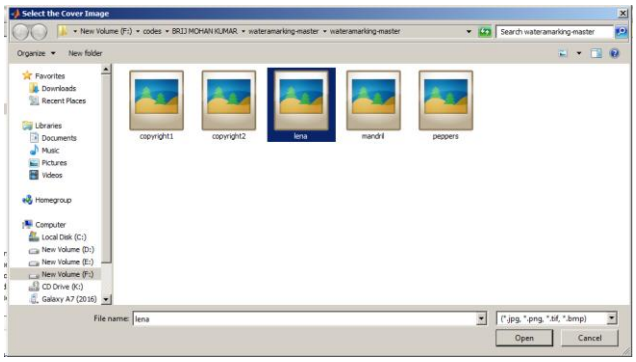

Figure 1: Select the cover image

2. Then the program prompts the user to select the image containing secret message

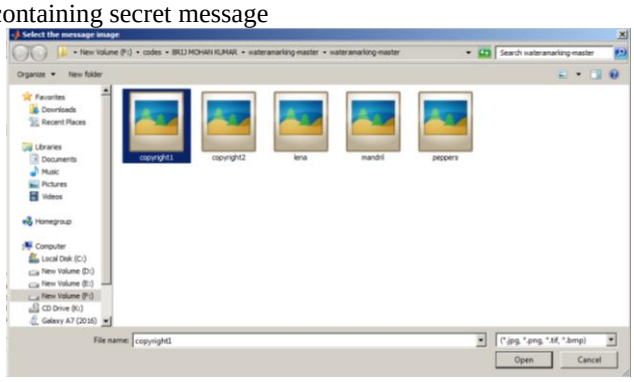

Figure 2: Select the secret message image

3. Then the program does the DWT decomposition as shown below

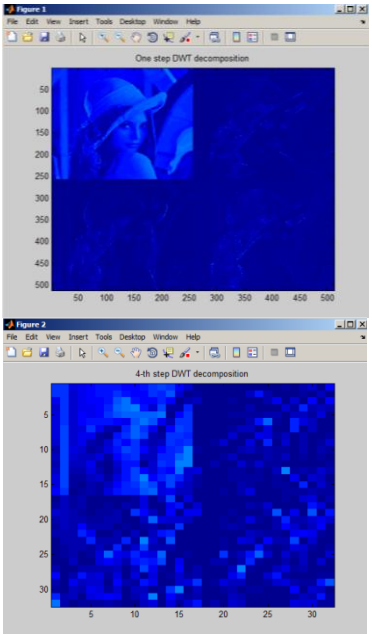

Figure 3: DWT decomposition

4. The complete process is as shown below

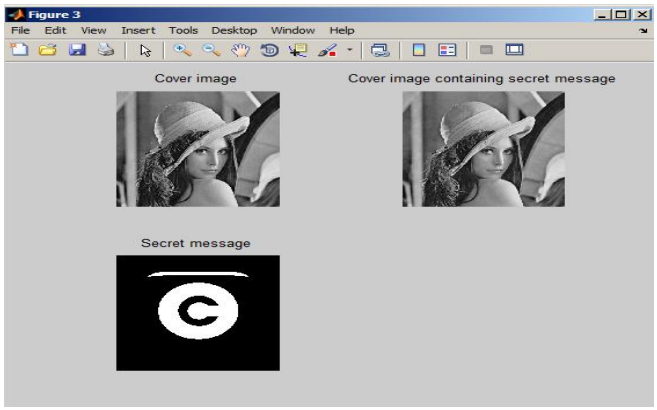

Figure 4: Final result

5. And finally the recovered secret message is displayed in a separate window

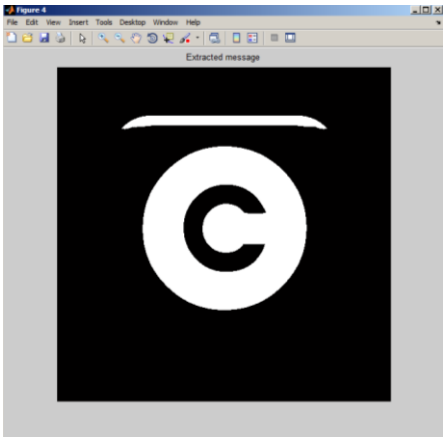

Figure 5: extracted secret message in form of image

5. Authentication in the Proposed Scheme

Zhang & Li (2005) observed an authentication problem in the basic SVD based approaches proposed by Zhou & Chen (2004) and Ganic & Ahmet Eskicioglu (2004). This section describes the common problem with majority of SVD-based schemes appearing in the state-of-art literature. The solution is proposed in the later half of the section. To demonstrate the problem, Zhang & Li (2005) set-up an experiment using two Lena images. Two different secret messages were embedded in them as shown in figure 2 using basic SVD scheme. The secret messages were embedded by modifying the singular values of Lena image with the singular values of the secret messages.

Decoder estimates the secret message by combining SV's extracted from one secret messaged image and using orthogonal matrices of other secret message. Figure 3 shows that the decoder extracted SV's from secret messaged image-2 and combine them with orthogonal matrices (U1 and V1) for secret message reconstruction. As a result, secret message-1 is recovered instead of secret message-2.

Thus we have performed the ROC (Receiver operating characteristics) test for our algorithm and the results are as under:-

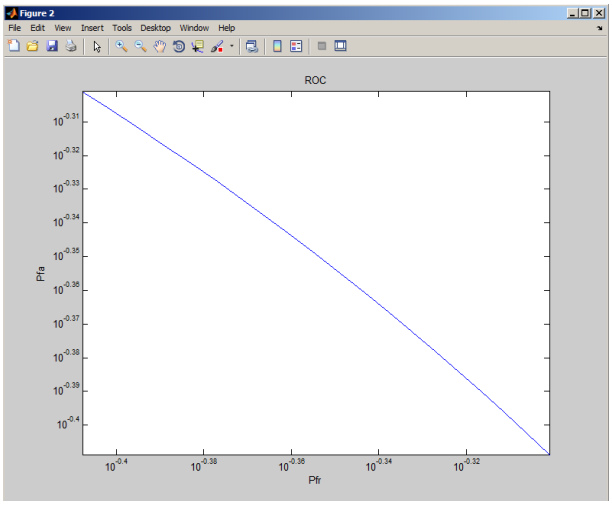

Figure 7: ROC curve for our algorithm

Moreover the secret message has also been reviewed in terms of Gaussian parameters which shows the degree of similarity between inserted and extracted message, it has been shown below

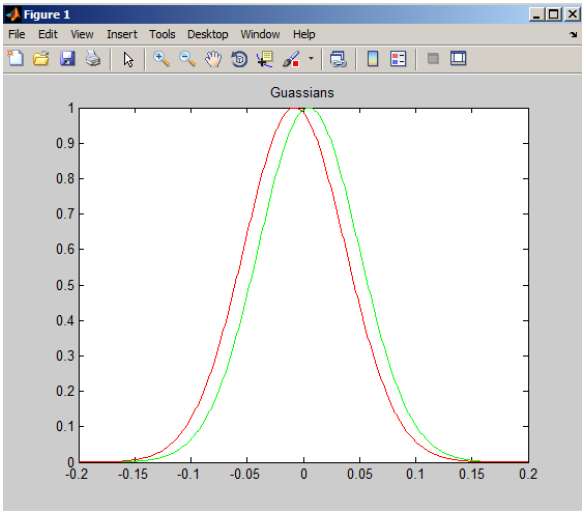

Figure 8: Gaussian curves for secret message

6. Conclusion

Our proposed scheme has high degree of robustness which is validated by recovering the secret message against print and scan attack which is among the strongest attacks. Even though scheme is blind in nature it gives result better than non-blind ones. Many of the existing DWT and SVD based approaches do not handle the issue of authentication and security. The proposed method covers this flaw by incorporating signature-based authentication mechanism. Thus the resultant method is both robust and secure.

References

[1] Andrews H C and Patterson C L 1976 Singular value decomposition (SVD) image coding. IEEE Trans. Comm. 24(4): 425–432
[2] Bhandari Kunal, Mitra Suman K and Jadhav Ashish 2005 A hybrid approach to digital image secret messageing using singular value decomposition and spread spectrum. S K Pal et al (eds): PreMI, LNCS 3776: 272–275
[3] Chen T S, Chang C C and Hwang M S 1998 A virtual image cryptosystem based upon vector quantization. IEEE Trans. Image Process. 7(10): 1485–1488
[4] Ganic Emir and Ahmet Eskicioglu M 2004 Robust DWT-SVD domain image secret messaging: Embedding data in all frequencies. Proceedings of the workshop on Multimedia and Security 166–174
[5] Ghazy R A, El-Fishawy N A, Hadhoud M M, Dessouky M I and El-Samie F E A 2007 An efficient blockby-block SVD-based image secret messaging scheme. Radio Science Conference, NRSC 1–9
[6] Kasmani S A and Naghsh-Nilchi A 2008 A new robust digital image secret messaging technique based on joint DWT-DCT transformation. Convergence and Hybrid Information Technology ICCIT ‘08 Third International Conference 2(1): 539–544
[7] Katzenbeisser Stefan and Petitcolas Fabien A 2000 Information hiding techniques for steganography and digital secret messaging. Norwood, MA, USA: Artech House, Inc.
[8] Lee Sin-Joo and Jung Sung-Hwan 2001 A survey of secret messaging techniques applied to multimedia. industrial electronics. Proceedings. ISIE 2001. IEEE International Symposium pp.272–277
[9] Liu R and Tan T 2002 A SVD-based secret messaging scheme for protecting rightful ownership. IEEE Trans. Multimed. 4(1): 121–128
[10] Podilchuk C I and Delp E J 2001 Digital secret messaging: Algorithms and applications. Signal Process. Mag. IEEE. 18(4): 33–46
[11] Quan Liu and Qingsong Ai 2004 Combination of DCT-based and SVD-based secret messaging scheme. Signal Processing Proceedings, ICSP ‘04, 7th International Conference pp. 873–876
[12] Raval M S and Rege P P 2003 Discrete wavelet transform based multiple secret messaging scheme. TENCON, Conference on Convergent Technologies for Asia-Pacific Region 3(1): 935–938
[13] Zhang Xiao-Ping and Li Kan 2005 Comments on-An SVD-based secret messaging scheme for protecting rightful ownership. Multimed., IEEE Trans. 7(3): 593–594
[14] Zhou B and Chen J 2004 A geometric distortion resilient image secret messaging algorithm based on SVD. Chin. J. Image Graphics. 9(1): 506–512