SVD-DWT Amalgamated Cryptography Scheme Antagonistic to Noise Attacks

Swati Dwivedi
M. Tech. Scholar
Computer Science and Engineering Department
Truba College of Science and Technology, Bhopal

Amit Saxena
Professor, Head of Department
Computer Science and Engineering Department
Truba College of Science and Technology, Bhopal

ABSTRACT

In order to improve the robustness and imperceptibleness of the algorithm, a new embedding and extracting method with DWT-SVD is proposed. The approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient. The proposed embedding and extracting method was employed to accelerate the hybrid DWT-SVD cryptography and to avoid the leak of watermark. This hybrid technique leads to optimize both the fundamentally conflicting requirements. The experimental results show both the good robustness under numerous attacks and the high fidelity. The time needed to perform the program is greatly decreased.

Keywords

Discrete Wavelet Transform, SVD, PSNR, MSE

1. INTRODUCTION

In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Everybody can obtain copies of copyrighted multimedia openly. So we need to generate a robust method in order to protect the copy rights of media. Digital cryptography provides copyright protection of data. It is done by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to make an assertion about the multimedia data. [1, 2] For image cryptography, the algorithms can be categorized into one of the two domains: spatial domain or transform domain. [1, 2] In Spatial domain the data is embedded directly by modifying pixel values of the host image, while transform domain schemes embed data by modifying transform domain coefficients. Algorithms used for special domain are less robust for various attacks as the changes are made at least Significant Substitution (LSB) of original data. While in the transform-domain the watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD) techniques [3]. This provide most robust algorithm for many common attacks. [4] In this paper we proposed a hybrid cryptography using DWT and SVD technique in order to achieve high robustness and transparency.

Therefore we decided to design cryptography schemes such that an inherent nature in can be embedded to guarantee that at least one serious attack having most financial implications cannot be conducted on watermarked images**.** If owner identification applications place the same watermark in all copies of the same content, then it may create a problem. If out of n number of legal buyer of content, one starts to sell the contents illegally, it may be very difficult to know who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy [5].

This particular application area is known as fingerprinting and thus has numerous financial implications. The most serious attack for fingerprinting is the “collusion attack”. If attacker has access to more than one copy of watermarked image, he/she can predict/ remove the watermark data by colluding them. Researchers working on “fingerprinting” primarily focus on the “collusion attack” [6].

So, while designing a watermark scheme, we decided that our proposed schemes must be designed in such a way that schemes are inherently collusion attack resistant. Therefore this thesis presents a new term “ICAR (Inherently Collusion Attack Resistant)” as a requirement for a cryptography system. The other 3 issues are taken into account while developing the cryptography schemes [7, 8].

The first chapter is devoted to the introduction of the cryptography area. Data hiding background is represented and the related terminologies are explained. Then various application areas of cryptography are represented and what may the key requirements of a successful cryptography system are discussed. Since cryptography can be classified on various parameters, the various types of cryptography are represented based on different classifications [9].

ISSUE 1: Till now there is no “Generic” nature in the cryptography algorithms available. More precisely, if certain approach is applicable for a gray level image, the same approach does not work for the other formats of an image [10].

ISSUE 2: Even if gray color image cryptography algorithms are extended for RGB color images, the maximum work has been done for BLUE color channel only because human eyes are less sensitive to detect the changes in BLUE color channel. No attack impact analysis, i.e, which color channel may be affected by a particular attack, has been carried out.

Therefore, apart from choosing digital Image Cryptography as a major problem, we have chosen to identify the suitability of a color channel with respect to attack (if any) for multicolor channel images (True color windows BMP, uncompressed JPEG). We also decided to explore the ways such that attack impacts may be minimized before the watermark embedding process [11]**.**

ISSUE 3: In most of the research papers, once the cryptography scheme is finalized, it is applied to all test images. Since each image is different and has certain characteristics and after embedding the watermark data by a particular cryptography scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics.

2. DIGITAL CRYPTOGRAPHY

The data to be inserted in a flag is known as an advanced watermark, despite the fact that in a few settings the expression computerized watermark implies the distinction between the watermarked flag and the cover flag. The flag where the watermark is to be implanted is known as the host flag. A cryptography framework is typically isolated into three unmistakable advances, inserting, assault, and recognition. In inserting, a calculation acknowledges the host and the information to be implanted, and creates a watermarked flag.

At that point the watermarked advanced flag is transmitted or put away, generally transmitted to someone else. On the off chance that this individual makes an alteration, this is called an assault. While the adjustment may not be malignant, the term assault emerges from copyright insurance application, where outsiders may endeavor to expel the advanced watermark through change. There are numerous conceivable changes, for instance, lossy pressure of the information (in which determination is decreased), editing a picture or video, or deliberately including clamor.

Recognition (regularly called extraction) is a calculation which is connected to the assaulted flag to endeavor to remove the watermark from it. In the event that the flag was unmodified amid transmission, at that point the watermark still is available and it might be removed. In vigorous advanced cryptography applications, the extraction calculation ought to have the capacity to deliver the watermark accurately, regardless of whether the adjustments were solid. In delicate advanced cryptography, the extraction calculation ought to fizzle if any change is made to the flag.

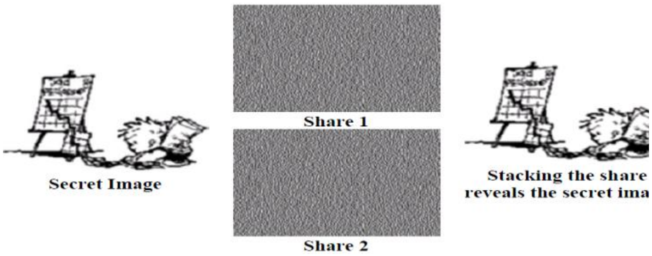

Figure 1: Visual Cryptography – An Example

3. DISCRETE WAVELET TRANSFORM

The model used in [5] to implement the tree structure of Direct Wavelet Transform (DWT) is based on the filtering process. Figure 1 depicted a complete 2-level Direct WT. In this figure G and H is the high pass and low pass filter respectively.

Computation period is the number of the input cycles for one time produces output samples. In general, the computation period is M= for a j-level DWT. The period of the 2-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N- sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies π/2 to π rad/s (hence double the frequency resolution).

The output of the low-pass filer also has N/2- sample points, but it spans the other half of the frequency band, frequencies from 0 to π/2 rad/s. Again low and high-pass filter output passed through the same low pass and high pass filters for further decomposition. The output of the second low pass filter followed by sub sampling has N/4 samples spanning a frequency band of 0 to π/4 rad/s, and the output of the second high pass filter followed by sub sampling has N/4 samples spanning a frequency band of π/4 to π/2 rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this specific example there would be 3 levels of decomposition, each having half the number of samples of the previous level.

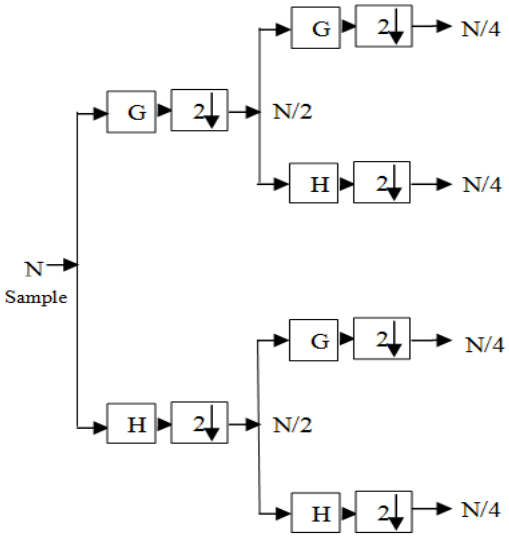

Figure 2: 2- Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient

The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal.

4. PROPOSED METHODOLOGY

DWT involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DWT is implemented as multistage transformation. Level wise decomposition is done in multistage transformation.

S is a diagonal matrix of singular values in decreasing order. The basic idea behind SVD technique of cryptography is to find SVD of image and the altering the singular value to embed the watermark. In Digital cryptography schemes, SVD is used due to its main properties:

1) As mall agitation added in the image, does not cause large variation in its singular values.

2) The singular value represents intrinsic algebraic image properties. [3]

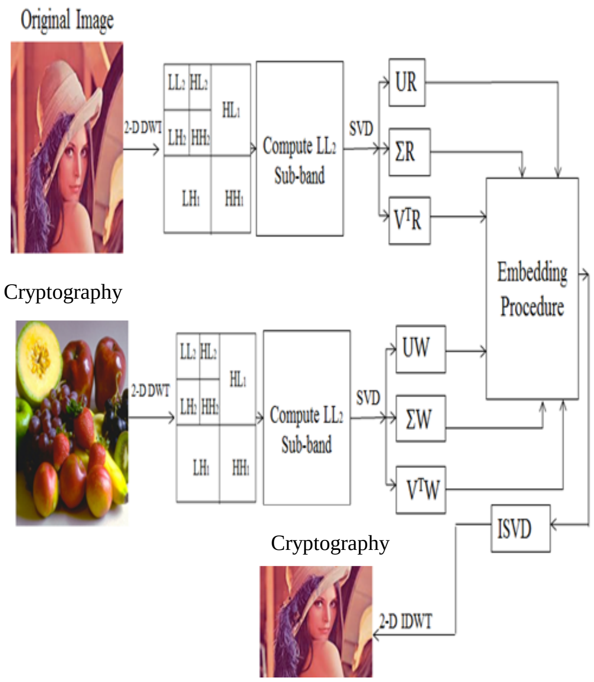

Figure 3: Flow Chart of Proposed Methodology

Algorithm for Cryptography Embedding

Step 1: Take host image as input and convert it into Rearrange image original (RIO).

Step 2: Apply 2-D DWT on rearranged image original (RIO) to decompose it into seven sub-bands.

Step 3: Select sub-band LL$_2$ of RI.

Step 4: Then apply SVD to sub-bands LL$_2$ to get UR, ΣR and V^{T}R.

Step 5: Take watermark image as input and convert it into Rearrange image watermark (RIW). Apply 2-D DWT on rearranged image watermark (RIO) to decompose into seven sub-bands.

Step 6: Select sub-bands LL$_2$ of Wi.

Step 7: Then apply SVD to sub-bands LL$_2$ to get UW, ΣW and V^{T}W.

Step 8: Modify UR, ΣR and V^{T}R by using equation

$UR^* = UR + (0.10*UW);$

$\Sigma R^* = \Sigma R + (0.10* \Sigma W);$

$V^TR^* = V^TR +(0.10* V^TW);$

Step 9: Construct modified SVD matrix UR*, ΣR* and V^{T}R*.

Step 10: Apply inverse SVD.

Step 11: Apply inverse DWT and finally get watermarked image WI.

5. SIMULATION RESULT

Discrete Wavelet Transform (DWT): The digital wavelet transform are scalable in nature. DWT more frequently used in digital image cryptography because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently.

Singular value decomposition (SVD): Singular value decomposition is a linear algebra technique used to solve many mathematical problems. Any image can be considered as a square matrix without loss of generality. So SVD technique can be applied to any kind of images. The SVD belongs to orthogonal transform which decompose the given matrix into three matrices of same size.

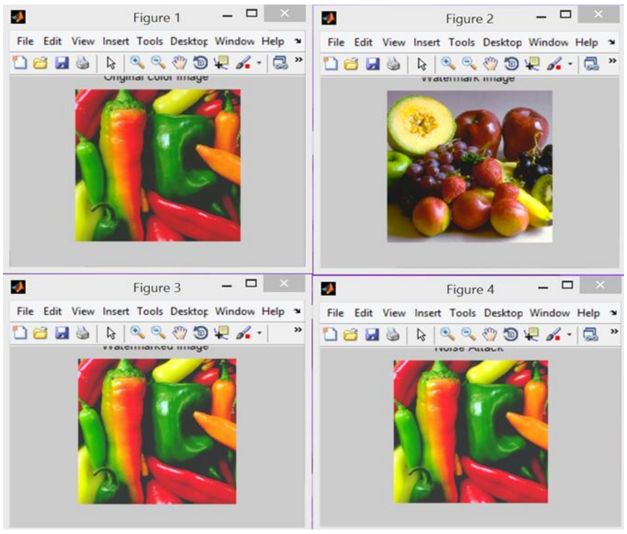
Figure 1
File Edit View Insert Tools Desktop Window Help
Original color image
Figure 2
File Edit View Insert Tools Desktop Window Help
Watermark image
Figure 3
File Edit View Insert Tools Desktop Window Help
Watermarked image
Figure 4
File Edit View Insert Tools Desktop Window Help
Noise Attack

Figure 4: DWT-SVD Technique are applied to the Peppers Image

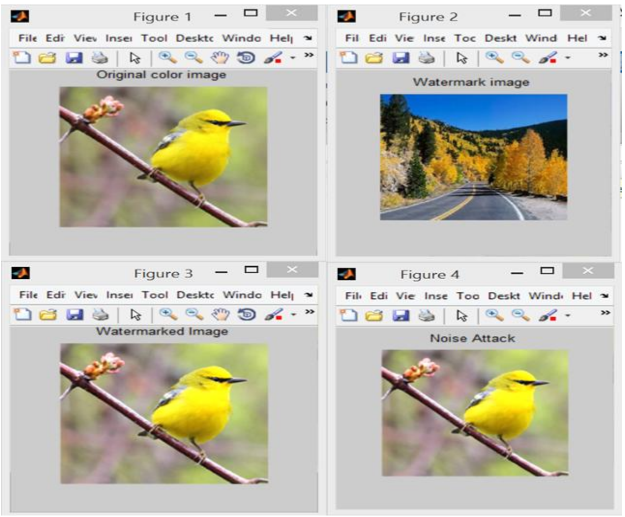
Figure 1
File Edi Viev Inse Tool Desktc Windo Help
Original color image
Figure 2
Fil Edi Vie Inse Toc Deskt Wind Hel
Watermark image
Figure 3
File Edi Viev Inse Tool Desktc Windo Help
Watermarked Image
Figure 4
Fil Edi Vie Inse Too Deskt Wind Hel
Noise Attack

Figure 5: DWT-SVD Technique are applied to the Flower Image

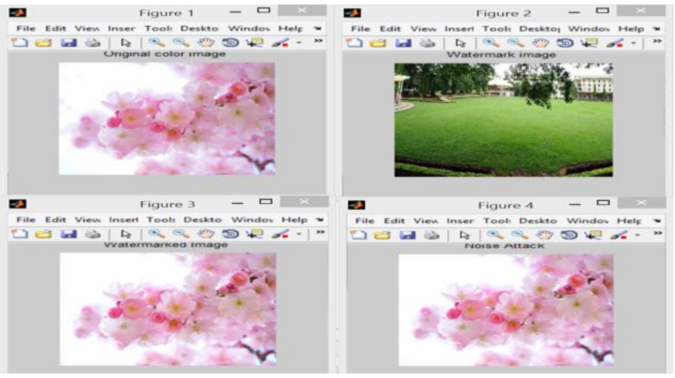
Figure 1
File Edit View Inser Tool Deskto Window Help
Original color image
Figure 2
File Edit View Insert Tools Desktop Window Help
Watermark image
Figure 3
File Edit View Insert Tools Deskto Window Help
Watermarked image
Figure 4
File Edit View Inser Tools Deskto Window Help
Noise Attack

Figure 6: DWT-SVD Technique are applied to the Green Image

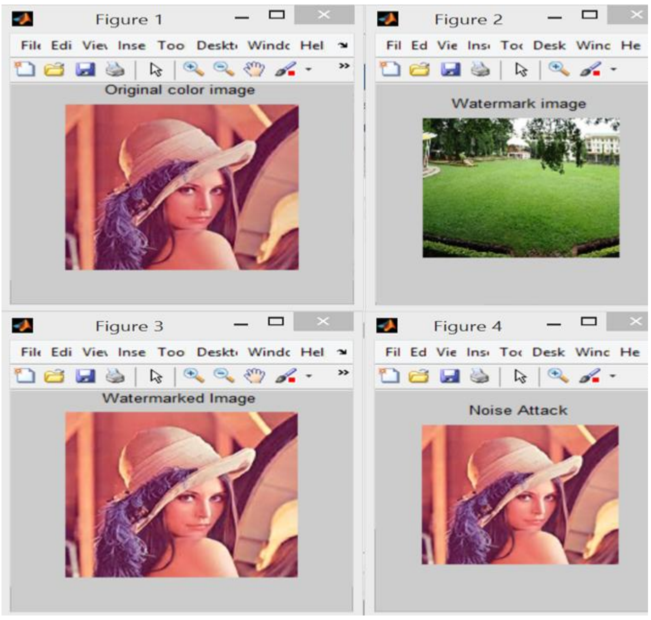

Figure 7: DWT-SVD Technique are applied to the Lena Image

Table 1: Result Obtained Without Attack

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
Host Image	32.702	24.059	4.904	8.032	4.04
Bird Image	33.101	23.082	4.804	7.704	4.98
Flower Image	32.078	22.912	4.786	7.521	4.73
Lena Image	33.094	22.740	4.768	8.226	4.64
Tree Image	32.704	22.062	4.697	8.476	4.40

Table 2: Result Obtained Gaussian Noise Attack

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
Host Image	29.864	25.7597	8.3286	9.241	4.451
Bird Image	30.865	22.2821	7.4443	6.702	3.145
Flower Image	28.765	19.4129	5.2992	4.962	5.347
Lena Image	30.654	22.543	6.954	3.654	4.332
Tree Image	31.432	25.782	8.543	3.576	3.667

Table 3: Result Obtained Salt and Pepper Noise Attack

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
Host Image	34.702	24.059	4.904	8.032	4.04
Bird Image	34.501	23.082	4.804	7.704	4.98
Flower Image	34.278	22.912	4.786	7.521	4.73
Lena Image	34.194	22.740	4.768	8.226	4.64
Tree Image	33.804	22.062	4.697	8.476	4.40

Table 4: Result Obtained Gaussian Localvar Noise Attack

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
Host Image	32.804	24.859	4.985	8.242	4.89
Bird Image	31.805	19.982	4.470	8.704	4.03
Flower Image	32.098	17.412	4.172	7.961	4.34
Lena Image	32.094	18.540	4.305	7.656	4.93
Tree Image	31.904	22.082	4.699	8.576	3.96

Table 5: Result Obtained Poisson Noise Attack

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
Host Image	33.902	23.759	4.874	7.893	4.89
Bird Image	32.901	21.982	4.688	7.904	4.43
Flower Image	33.078	20.412	4.517	7.021	4.84
Lena Image	34.094	21.540	4.641	7.226	4.63
Tree Image	33.604	21.082	4.591	7.976	4.26

6. CONCLUSION

It has been proved that the use of DWT-SVD with fusion method has improved the security of the cryptography scheme. Particular attention is given to the proposed scheme to guarantee secure watermark embedding and easy extraction. The watermark is imperceptible to the human eye and recoverable most of the time. The watermarked images were assessed for fidelity by using PSNR and MSE. The new techniques could offer significant advantages to the digital watermark field and provide additional benefits to the copyright protection industry.

7. REFERENCES

[1] N. Senthil Kumaran, and S. Abinaya, “Comparison Analysis of Digital Image Cryptography using DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[2] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[3] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Cryptography for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[4] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Cryptography Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[5] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[6] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image cryptography based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.

[7] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp. 86-106.

[8] Baaziz, N., Zheng, D. and Wang, D. (2011) Image quality assessment based on multiple cryptography approach, IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5.

[9] Bao, F., Deng, R., Deing, X. and Yang, Y. (2008) Private Query on Encrypted Data in Multi-User Settings, Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.

[10] Barni, M. and Bartolini, F. (2004) Cryptography systems engineering: Enabling digital assets security and other application, Signal processing and communications series, Marcel Dekker Inc., New York.

[11] Barni, M., Bartolini, F. and Piva, A. (2001) Improved Wavelet based Cryptography Through Pixel-Wise Masking, IEEE Transactions on Image Processing, Vol. 10, Pp. 783-791.