ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

A Semi Fragile Watermarking Algorithm Based on SVD-IWT for Image Authentication

U. M. Gokhale [1], Y.V.Joshi[2]
G.H.Raisoni Institute of Engineering and Technology for women, Nagpur (MS), India,
Walchand College of Engineering Sangli (MS), India

ABSTRACT— *A semi fragile watermarking algorithm based on image scrambling and SVD in the wavelet domain has been presented in this paper. In the proposed algorithm, chaotic signals are generated using logistic mapping and are used for scrambling the original watermark. The initial values of logistic mapping are taken as private keys. The covert image is decomposed into four sub bands using integer wavelet transform; we apply SVD to each sub band, embed the scrambled watermark data by modifying the singular values. Modification in all frequencies allows the development of a robust watermarking scheme that is robust to a wide range of attacks.*

Keywords— logistic mapping, Singular value Decomposition, Integer wavelet transform, Image authentication,

I. Introduction

In recent years, the rapid expansion of the interconnected networks and development of digital technologies have facilitated instant multimedia transmission and creation of large scale image databases. Recent advances in communication infrastructure, signal processing and digital storage technologies have enabled pervasive digital media distribution. Digital distribution introduces a flexible and cost effective business model that is beneficial to multimedia commerce transaction. The digital nature also allows individuals to manipulate, duplicate or access media beyond the conditions agreed upon for a given transaction. With some powerful software one can remove/replace some features in a digital image without any detectable trace. These kinds of operations are regarded as tampering. For medical, military and judicial applications such operations are not allowed. Under these conditions authentication has become an important issue in the digital world. Authentication is the service of ensuring whether a given block of data has integrity and is from legitimate sender [1].

Image authentication can be divided into two groups: strict and selective authentication. Strict authentication is used for applications where no modifications in the protected image are allowed. On the other hand, selective authentication is used especially when some image processing operations are to be tolerated. Selective authentication uses techniques based on semi fragile watermarking or image content signatures to provide some kind of robustness against specific and desired manipulations. Existing watermarking schemes can be divided into two categories spatial domain and transform domain. Spatial domain techniques embed data by directly modifying pixel values of the host image, while transform domain techniques embed data by modifying transform domain coefficients. Discrete cosine transform (DCT) and discrete wavelet transform (DWT), which are used in image compression standards JPEG and JPEG2000 respectively, are two main transforms used in transform domain watermarking. However, transform methods attempt to decompose images in terms of a standard basis set. This is not necessarily the optimum set. Recently Singular value decomposition (SVD) has been used for implementation of watermarking algorithms [2-11].

II. The Related Work :

In [1] Gorodetski et al. embed watermark bits by modifying the quantized singular values of the host image. In [2], Chandra computed SVD of both the host and watermark images and then singular values of the watermark images are minified and added to those of the host image. In [3] Liu and Tan applied SVD to only host image and watermark bits are directly added to its singular values. In [4] Ganic et al. propose a two layer watermarking scheme. In [5] A. Sverdlov et. al. Used SVD with DCT and in [6] E. Gagnic et. al. use SVD with DWT embedding data in all frequencies. In [7] Agrawal et al. propose a scheme of modifying the singular vectors instead of singular values. In [8] Ghazy et al. proposed a scheme in which the image is divided into blocks and then watermark is embedded in singular values of each block separately. In [9], W. Li et. al. used SVD with a human visual system (HVS) model.

In [11], however, it is demonstrated that a counterfeit attack on SVD watermarked image is possible and proposes a method to counter attack it. In [12, 13] it is pointed out that

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

SVD watermarking suffers from false watermark detection. In [14] it has been shown that SVD based watermarking based on combination of discrete wavelet transform (DWT) and vector transform (VT). Khaled et.al.[16] proposed hybrid watermarking algorithm based on SVD and Lifting wavelet transform for ownership verification. However the results are not encouraging for certain attacks such as median filtering. Thus SVD based watermarking methods cannot be used for the ownership verification of an image. In the proposed scheme watermarking is used for image authentication.

A. Singular Value Decomposition

Let A be an image matrix of size N×N. Using SVD the matrix A can be decomposed as:

$$A = U_A S_A V_A^T = \sum_{i=1}^{r} u_i \;\; s_i \, v_i^T \qquad (1)$$

with

$$U_A = [u_1, u_2, \ldots u_N] \qquad (2)$$

$$V_A = [v_1, v_2, \ldots v_N] \qquad (3)$$

$$S_A = \begin{bmatrix} s_1 & 0 \cdots 0 \\ 0 & s_2 \cdots 0 \\ \vdots \; \vdots & \ddots \;\; \vdots \\ 0 & 0 \cdots \; s_N \end{bmatrix} \qquad (4)$$

Where r is the rank of matrix A(r ≤ N), U_A and V_A are orthogonal matrices of size N×N, whose column vectors are u_i and v_i.. S is an N×N diagonal matrix containing the singular values s_i assumed to be in decreasing order.

In watermarking applications, SVD has following properties:

a) SVD is able to efficiently represent the intrinsic algebraic properties of an image, where singular values correspond to the luminance of the image and singular vectors reflect geometry characteristics of the image.

b) Singular values have good stability, which means small perturbation added to image will not significantly change the corresponding singular values.

c) An image matrix has many small singular values compared with the first value. If these values are ignored it will have much effect on the quality of reconstructed image.

B. Image Encryption

Chaos signal are a kind of pseudorandom, irreversible and dynamical signals generated by deterministic non linear equations, which possess good characteristics of pseudorandom sequences. There are many ways to generate chaos sequence. We use logistic mapping chaos sequence. The equation for logistic mapping chaos is given by equation (5).

$$X(n+1) = \mu X(n)\big(1 - X(n)\big) \qquad (5)$$

algorithms are robust to distortions as long as attacks are not severe. Xianghong et al [15] proposed a watermark scheme Where $0 \le \mu \le 4$, is called as branch parameter, x ϵ (0, 1). Logistic map is chaotic when $3.569945 \le \mu \le 4$, chaotic systems are highly sensitive to initial parameters.

In order to get chaotic sequence, the chaotic signal x (n+1) must be transformed into binary sequences. We use the logistic map to generate sequence W (i) using

$$W(i) = \begin{cases} 1, & W_i > T \\ 0, & W_i < T \end{cases} \qquad (6)$$

after appropriately selecting the threshold T.

Make the xor operation between the sequence and the matrix of the original watermark to obtain the scrambled watermark or encrypted watermark.

Fig. 1 shows the original and the encrypted watermark.

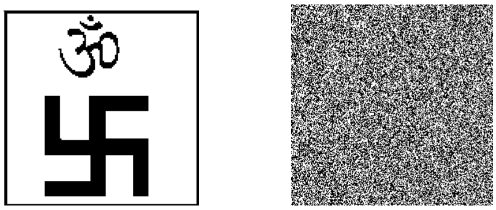


Fig. 1 a) Original Watermark b) Scrambled Watermark

III. THE PROPOSED METHOD

Proposed method is explained in the following section

A. Watermark embedding

The watermark embedding algorithm is as follows:

1) Using the integer DWT, cover image A is first decomposed into four sub bands LL, HL, LH, HH as shown in Fig. 2.

$$A \rightarrow I_s \;\; (s \in (LL, HL, LH, HH) \qquad (7)$$

2) Apply SVD to each sub band image :

$$I_S \rightarrow U_s S_s V_s^T \qquad (8)$$

3) Obtain the scrambled or encrypted image from the original image by using logistic mapping as described in section 2.

$$W = W(i) \; xor \; K \qquad (9)$$

Where K is the original watermark and W(i) is the chaotic sequence obtained by logistic mapping.

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

4) *Apply SVD to the encrypted image.*

$$W \rightarrow U_w S_w V_w^T \qquad (10)$$

5) *Modify the singular values of the cover image in each sub band with singular values of the encrypted watermark;*

$$\widehat{I_s} \rightarrow U_s\,(S_s + \alpha S_w)V_s^T \qquad (11)$$

6) *Obtain the four sets of modified DWT coefficients*

7) *Apply the inverse DWT using the four sets of modified DWT coefficients to produce the watermarked cover image.*

$$\hat{A} \leftarrow \widehat{I_s} \qquad (12)$$

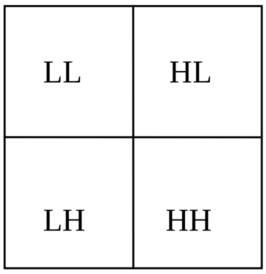


Fig 2 DWT decomposition of cover image

B. Watermark detection

The watermark detection algorithm is as follows

1. *Using Integer LWT, decompose the watermarked (and possibly attacked) cover image $\hat{A}$ into four sub bands LL, HL, LH, HH as shown in Fig 2.*

$$\hat{A} \rightarrow \hat{I}_s \;\; (s \in\; LL, HL, LH, HH) \qquad (13)$$

2. *Apply SVD to each sub band image :*

$$\hat{I}_s \rightarrow \widehat{U}_s \hat{S}_s \hat{V}_s^T \qquad 14)$$

3. *Extract the singular values from each sub band.*

$$\hat{S}_{ws} \leftarrow \frac{\hat{S}_s - S_s}{\alpha} \qquad (15)$$

4. *Construct four watermark images from four sub bands.*

$$W_s \rightarrow U_w \hat{S}_{ws} V_w^T \qquad (16)$$

5. *The original watermark can be obtained by xor operation with the chaotic sequence W (i).*

$$K_e = W(i)xor\;W_s \qquad (17)$$

The experimental simulation is carried out using MATLAB. The standard test images of 512×512×8 greyscale were used for studying the effects of perceptibility and robustness of the watermarking algorithm on a 256 × 256 binary watermark image. The images Lena, Baboon, Peppers, Plate, Tiffney, boat are shown in figure 2.In order to evaluate the difference between cover image and watermarked image, Mean square error (MSE) is used and Peak Signal to Noise Ratio (PSNR) is used to estimate the watermark imperceptibility.

$$PSNR = 10log10\left(\frac{255 * 255}{MSE}\right) \qquad 18)$$

Where, MSE is the Mean Square Error between the original and watermarked image.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}[\{x(i,j) - y(i,j)\}^2] \;(19)$$

Where x(i, j) and y(i, j) represent the pixel value of the original and the watermarked image respectively. A higher PSNR indicates that the quality of the watermarked image is closer to the original image. Fig. 2 shows the original cover images.

Fig. 2: Original Cover images

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

We estimate the similarity between the original watermark and the extracted watermark using normalized correlation (NC):

$$NC = \frac{\sum_{i=1}^{L} w(i) \times \hat{w}(i)}{\sqrt{\sum_{i=1}^{L} w(i)^2}\sqrt{\sum_{i=1}^{L} \hat{w}(i)}} \qquad (20)$$

The NC shows the robustness of the algorithm. Its value is 1.0000 before the watermark image is attacked.

In table I, The PSNR values are provided for standard images. It is observed that the PSNR values are quite high indicating good imperceptibility.

TABLE I
PSNR AND NC VALUES FOR DIFFERENT COVER IMAGES

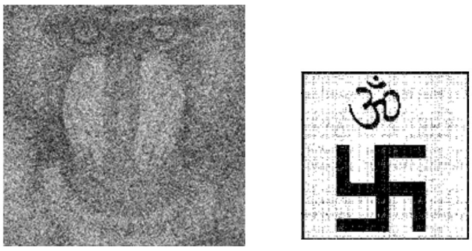
Image	PSNR in dB	NC		
		LH	HL	HH
Lena	50.4488	1	1	1
Baboon	49.7415	1	1	1
Peppers	50.5571	1	1	1
boat	49.7132	1	1	1
Tiffney	51,2245	1	1	1
Plate	51.1329	1	1	1

Table II shows the experimental results for proposed watermarking algorithm against various attacks when the watermark is embedded in the selected sub band LL,LH,HL,HH.Figure 3 shows Watermarked image attacked and extracted watermark under various attacks.
The first test is robustness to additive noise. Two kind of noise are tested. One is 30% salt & pepper noise and the other is zero mean Gaussian noise with variance 0.5, the result demonstrates that the proposed algorithm is robust to additive noise.
The algorithm is tested for image processing techniques such as sharpening filter and histogram equalization. The results show that the algorithm is robust against both the techniques.
In order to increase the robustness of the algorithm against median filter, Gaussian blur, rotation and gamma correction the watermarking strength is increased. The results are given in table III

Comparison with other Algorithms

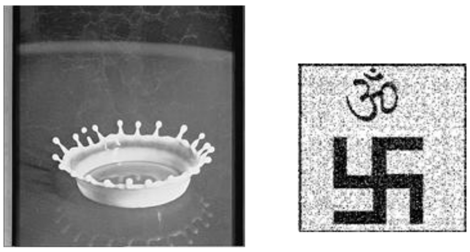
We compare our results with Xianghong and et al [15] and Khaled and et al.[16].Figure4 shows the normalized correlation (NC) comparison between proposed scheme and the other two schemes. In this comparison we have used Peppers as cover image and LH sub band for four attacks. The results obtained indicate that our algorithm performs best in terms of robustness.

(a)Salt & Pepper noise (Density=0.3, NC=1)



(b)Gaussian noise (mean 0, Var=0.5, NC=0.9713

(c) Histogram equalization (NC=0.9859)



(d) Sharpening (NC=0.9195)

Fig3 Watermark image attacked and Extracted watermark

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

Table II (a) Salt & Pepper noise (Density =0.3)

Image	LL	LH	HL	HH
Lena	0.9122	1.0000	1.0000	1.0000
Baboon	0.9527	1.0000	1.0000	1.0000
Peppers	0.8815	1.0000	1.0000	1.0000
Plate	0.9832	1.0000	1.0000	1.0000
Tiffney	0.8848	1.0000	1.0000	1.0000
Boat	0.9051	1.0000	1.0000	1.0000

Table II (b) Gaussian Noise (M=0, V=0.5)

Image	LL	LH	HL	HH
Lena	0.9297	1.0000	1.0000	1.0000
Baboon	0.9706	1.0000	1.0000	1.0000
Peppers	0.8914	1.0000	1.0000	1.0000
Plate	0.9892	1.0000	1.0000	1.0000
Tiffney	0.7862	1.0000	1.0000	1.0000
Boat	0.9139	1.0000	1.0000	1.0000

Table II (c) Histogram Equalization

Image	LL	LH	HL	HH
Lena	0.8647	1.0000	0.9997	1.0000
Baboon	0.9634	1.0000	1.0000	1.0000
Peppers	0.8228	0.9859	0.9999	0.9983
Plate	0.6214	0.9986	0.6298	1.0000
Tiffney	0.6390	1.0000	0.9996	1.0000
Boat	0.8290	1.0000	1.0000	0.9905

Table II (d) Sharpening attack

Image	LL	LH	HL	HH
Lena	0.9297	1.0000	1.0000	1.0000
Baboon	0.9706	1.0000	1.0000	1.0000
Peppers	0.8914	1.0000	1.0000	1.0000
Plate	0.9892	1.0000	1.0000	1.0000
Tiffney	0.7862	1.0000	1.0000	1.0000
Boat	0.9139	1.0000	1.0000	1.0000

Table III Test with increased watermarking strength

Attack	LL	LH	HL	HH
Median filter	0.8600	0.6233	0.6233	0.6233
Gaussian Blur (3×3)	0.9900	0.6233	0.6233	0.5754
Rotation 2^0	0.8277	0.7700	0.6348	0.6233
Gamma Correction (0.8)	0.6214	1.0000	1.0000	1.0000

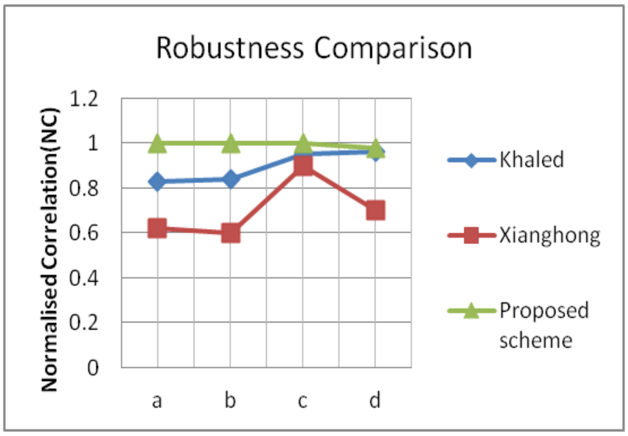


Figure 4 Robustness comparisons.
(a) Salt & Pepper noise 30%;(b) Gaussian noise(0,0.5);(c)Sharpening;(d)Histogram Equalization

Table IV presents a comparison in terms of Imperceptibility: propose algorithm clearly outperforms the Xianghong and et al. Method but is close to Khaled and et al. method in terms of visual quality of watermarked image.

TABLE IV: IMPERCEPTIBILITY COMPARISON

Image	Proposed Method PSNR(dB)	Xianghong PSNR(dB)	Khaled PSNR(dB)
Lena	50.44	35.84	52.76
Baboon	49.74	35.93	52.64
Peppers	50.55	35.74	53.03
Boat	49.71	35.87	53.03

IV. CONCLUSIONS

The proposed watermarking algorithm is *non-blind* watermarking technique as the original image is required for the watermark extraction. The PSNR is around 50dB before the attacks. The robustness against many attacks is very good. In the existing watermarking algorithms there is always a trade off between higher robustness and degree of perceptibility. The proposed algorithm achieves both high robustness and imperceptibility. The security of the watermark is improved by its encryption using the chaos sequence generated by logistic mapping.

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

REFERENCES

1. V.Gorodetski, L. Popyack, V. Samoilov and V. Skormin, " SVD based approach to transparent embedding data into digital images," in proc. International Workshop on mathematical methods, model and architectures for computer network security (MMM-ACNS'01), may 2001
2. Chandra D.V.S.; "Digital image watermarking using singular value decomposition", Circuits and Systems 2002.MWSCAS-2002, vol.3, 4-7Aug 2002, pp. 264-267.
3. R. Liu, T. Tan, "An SVD –based watermarking scheme for protecting rightful ownership", *IEEE Transaction on* Multimedia Volume 4, issue 1, March 2002 pp121-128.
4. E.Gagnic, N. Zubair and A.M.Eskicioglu, "An optimal Watermarking based on singular value decomposition,"in proc *IASTED international Conference on Communication , network and Information security(CNIS'03),*Dec.2003
5. A.Sverdlov, S. Dexter and A.M.Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection : Embedding data in all frequencies, in proc. the 2004 Multimedia and Security Workshop, ACM press, sep 2004,pp. 166-174.
6. E. Gagnic and A.M. Eskicioglu, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition", Journal of Electronic Imaging vol. 14, no.4, Dec 2005.
7. R.Agrawal and M.S.Santhanam, "Digital watermarking in the singular vector domain,"Mar.2006.
8. R.A.Ghazy, N.A El-Fishawy, M. M Hadhoud, M.I.Dessouky and F.E. Abd El-Samie, "An efficient Block by block SVD based image watermarking scheme", Ubiquitous computing and communication Journal ,2(5),2007,pp. 1-9.
9. Q.Li, C. Yuan and Y.Z. Zhong, "A novel SVD based watermarking scheme using human visual model," in Proc. The 2nd International Symposium on Computational intelligence and Industrial Applications, Nov 2006.
10. AndrewsH, Patterson C., "Singular Value Decomposition (SVD) Image Coding", *IEEE Transaction on [legacy, pre-1988], Volume 24, Issue 4, April 1976, pp425-432*.
11. Y.D.Wu, "On the security of an SVD-Based Ownership Watermarking, IEEE Transactions on Multimedia, 7 (4), August 2005, pp.624-627
12. X.P. Zhang, K.Li comments on "An SVD-Based Watermarking scheme for Protecting Rightful Ownership", IEEE Transaction on multimedia Vol.7,no.2,2005, pp.593-594.
13. R.Rykaczewski, comments on "An SVD-Based Watermarking scheme for Protecting Rightful Ownership", IEEE Transaction on multimedia Vol.9,no.2,2007,pp.421-423.
14. Xiong Changzhen, Guo Fenhong,Li Zhengxi, "Weakness Analysis of Singular Value based Watermarking", in proceedings of the 2009 IEEE international Conference on Mechtronics and Automation August 9-12, Changchun, China.
15. T. Xianghong ,L Li, L. Yang and Y Niu, "A digital watermarking scheme based on DWT and vector transform", International Sympo. On Intelligent multimedia, video and speech processing, pp.635-638, Hongkong, Oct 2004.
16. Khaled L. and J.Y.Chouinard," Hybrid watermarking algorithm based on SVD and Lifting wavelet Transform for ownership Verification, 11th Canadian workshop on information theory CWIT 2009.
17. U.M.Gokhale and Y.V. Joshi," A new watermarking algorithm based on image scrambling and SVD in the wavelet domain" in the Proc. of Int.Conf. on Advances in Computer Engineering 2011, pp 35-38.

Biography

U.M.Gokhale is presently working as Asst.Professor and Head in department of Electronics and Telecommunication in G.H.Raisoni Institute of Engineering and Technology for women, Nagpur (MS), India. He has 3 international journal publications and 5 national and international conference publications to his credit. He is Life member of Indian Society for Technical Education (ISTE). He has 22 years experience of teaching in Engineering College.

Dr. Y. V. Joshi is presently working as Director of Walchand College of Engineering, Sangli since May 2009. Earlier he was at SGGS Institute of Engineering and Technology, Vishnupuri, Nanded since 1986 in various capacities starting with Lecturer (1986-1993), Assistant Professor (1993-2001), Professor (2001 onwards).

He has 15 international Journal publications and 25 national and international conference publications to his credit. He is Life Member of ISTE. He conducts and supervises research in the areas of Signal and Image processing. He has supervised more than 25 M.E. /M.Tech dissertations and 3 Ph.D. students