International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 717-726

http://www. irphouse.com

A Robust Steganographic Method based on Singular Value Decomposition

Yambem Jina Chanu[1], Kh. Manglem Singh[2] and Themrichon Tuithung[3]

[1, 3] Dept. of CSE, NERIST, Itanagar ,
[2] Dept. of CSE, NIT Manipur ,

ABSTRACT

Many steganographic techniques have been produced for embedding secret message based on singular value decomposition (SVD) in last decades. These techniques embed message in either right singular vectors, left singular vectors, singular values or combinations of all approaches in spatial domain or transform domain with satisfactory performance to various attacks. The cover image may be divided into many blocks for embedding the secret message. Our steganographic method proposes a new method that first divides the image into many equal-size blocks and embeds the secret message in the singular values of the block of the image. The proposed method never assigns negative values in the singular values to embed secret message unlike the other existing methods. Experimental results show that the proposed method is robust against the various attacks.

Keywords- Steganography; SVD.

1. INTRODUCTION

The word steganography was derived from two Greek words steganos, meaning "covered," and graphein, meaning "to write"[H. Wang et al. 2004]. It refers to the technique of embedding secret messages inside different cover media such as text, audio, image and video without any suspicion. It can be used in many areas. The main purpose of steganography is to transmit hidden message embedded in a cover medium in a stealth way that an unauthorized person cannot extract the very presence of the embedded message. Generally steganography consist of three basic types: spatial steganography, transform steganography and adaptive steganography. SVD is one of the popular transform domain. Two contemporary SVD based steganography technique are also implemented, along with it we have implemented the method proposed by Chang et al (CM) [C-C. Chang et al., 2007] too. The first method is the one proposed by Bergman and Davidson (BM)[C. Bergman et al., 2005] where the

left singular vectors are modified for embedding secret messages. The second method is proposed by Yang et al (YM)[K-L. Chung et al., 2007] where the left singular vectors are modified, column wise without touching the diagonal values and the above portion of it. The performance of these three above mentioned SVD based steganography technique including the proposed method is evaluated in terms of normalized correlation (NC) and peak-signal-to-noise-ratio (PSNR). NC is used to evaluate the similarity between the original watermark and the revealed watermark. PSNR is used to evaluate the similarity of the original image and stego-image. Various types of attacks such as no attack, compression attack, cropping attack, impulse noise attack, Gaussian attack and gamma correction attack are used to test the robustness of the proposed method with the existing one. The rest of the paper is organised as follows Section 2, SVD review. Section 3, survey on different applications of SVD. Section 4, proposed method. Section 5, experimental results. Section 6, Conclusions and followed by Section 7, References.

2. SVD REVIEW

The singular value decomposition is a mathematical tool for analyzing a mapping from one vector space into another vector space, possibly with a different direction [L. Hogben et al., 2006]. The SVD is based on a theorem from linear algebra which says that a rectangular matrix A of $m \times n$ size can be factored into three matrices.

$$A = USV^T \tag{1}$$

where U is orthogonal $m \times m$ matrix $(U^TU = I)$ (where I is identity matrix) and the columns of U are the orthonormal eigenvectors of AA^T. Likewise V is orthogonal $n \times n$ matrix $(V^TV = I)$ and the rows of V^T are the eigenvectors of A^TA. The eigenvectors of AA^T are called the left singular vectors of U, while the eigenvectors of AA^T are called the right singular vectors of V. The matrix S is diagonal and it has the same size as A. Its diagonal entries, known as sigma, $\sigma_1, \dots, \sigma_r$, arranged in non-increasing order are the square roots of the nonzero eigenvalues $\lambda_1, \dots, \lambda_r$, where $\sigma_1 = \sqrt{\lambda_1}$,..., $\sigma_r = \sqrt{\lambda_r}$, of both AA^T and A^TA. They are the singular values of matrix A and they fill the first r places on the main diagonal of S. r is the rank of A. Singular value vector has the entire energy of the matrix A, U and V represent the geometrical shape of the image.

This is called singular value decomposition, because the factorization finds values or eigenvalues or characteristic roots that make the following characteristic equation singular. That is,

$$|AA^T - \lambda I| = 0 \tag{2}$$

This polynomial that yields n- roots, is called characteristic polynomial. Eq. (2) comes from a more generalized eigenvalue equation, which has the form

$$AA^T\boldsymbol{x} = \lambda\boldsymbol{x} \tag{3}$$

Equation 3 can be written in matrix form as

$$AA^T\boldsymbol{x} - \lambda\boldsymbol{x} = 0 \quad \text{or} \quad (AA^T - \lambda I)\boldsymbol{x} = 0 \tag{4}$$

This equation gives either $\boldsymbol{x} = 0$ or $|AA^T - \lambda I| = 0$.
Properties of the SVD are

- S is a diagonal matrix with real, nonnegative diagonal entries $\sigma_1, \sigma_2, \dots, \sigma_n$ such that $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n$. These singular values are unique.
- $AA^T = USS^TU^T$, it follows that U diagonalizes AA^T and the u_i's are the eigenvectors of AA^T.
- $A^TA = VS^TSV^T$, it follows that V diagonalizes A^TA and the v_i's are the eigenvectors of A^TA.
- The rank of A is equal to the number of nonzero singular values.
- The eigenvectors of U and V are not unique.
- If A has a rank of r, then $v_1, v_2, \dots, v_r$ form an orthonormal basis for the rank space A^T, $R(A^T)$, and $u_1, u_2, \dots, u_r$ form an orthonormal basis for the rank space $A, R\ (A)$.

3. SURVEY ON DIFFERENT APPLICATIONS OF SVD

Bergman and Davidson proposed a steganography technique that computed the SVD of submatrices of the image, then embeds the secret message in the left singular vectors [C. Bergman et al., January 2005]. Their algorithm is able to defeat some of the steganalytic statistical attacks, which analysed the pixel value directly. Hadhoud and Shallan proposed an image steganographic technique based on SVD that embedded the secret message in the left singular vectors, leaving untouched the diagonal matrix, for less embedding error and better image fidelity [M.M. Hadhoud et al. , 2009]. Chung et al developed an image hiding scheme based on the SVD and vector quantization (VQ) [K.L. Chung et al.,2001]. Their algorithm leads to good compression ratio and satisfactory image quality. Raja et al proposed robust and high capacity image steganography using SVD (RHISSVD), which embedded message bits in singular values of the cover image [K.B. Raja et al., 2008]. Gorodetski et al proposed a robust SVD-based steganography technique, which inserted message bits into singular values of small blocks of segmented cover image by slight modification [V.I Gorodetski et al., 2001]. The method is robust because it embeds data in low bands of cover in a distributed way. Chang et al proposed an information hiding technique that hid information in singular values of the SVD [C-C. Chang et al., 2007]. Chung et al presented two notes for singular value decomposition based watermarking scheme, which can increases the invisibility and capacity when embedding the information into left and right singular vectors of the SVD [K-L. Chung et al. ,2007]. A significant effort has been devoted to copyright protection in the SVD domain involving still images [R. Liu et al.,2002 , X. Zhang et al. 2005]. Haghighi and Ghaemmaghami used a linear programming method to embed information into the singular values of an image, while taking perceptibility into account [M. S. Haghighi et al.,2005]. Ganic and Eskicoglu used DWT-SVD-based technique that embedded information into the singular values of certain subbands from the DWT [E. Ganic et al.,2004]. Kaufman and Celenk proposed the SVD for the

video in discrete cosine transform [J. Kaufman et al., 2006]. Shieh et al proposed a semi-blind watermarking scheme based on singular value decomposition, which leads to satisfactory robustness to various attack [J-M. Shieh et al., 2006]. Hsu and Chen proposed SVD based projection for face recognition [C-H Hsu et al., 2007]. Their method required less space and more efficient than other eigenface methods based on principal component analysis. Zhang et al proposed SVD perturbation based method for face recognition [D.Q. Zhang et al., 2005]. Sharif et al proposed a face recognition method based on SVD, which can handle variation in light illumination and face expression [M. Sharif et al., 2012]. Sadek gave the weakness of SVD to vulnerability of singular values to a wide class of image processing operation as well as intentional attacks [R. A. Sadek 2008].

4. PROPOSED METHOD (PM)

The proposed SVD based steganographic method is the modification of the one proposed by Chang et al [C-C. Chang et al., 2007]. The unique property of singular values in SVD is that, they are non-negative. But Chang's method assigns some of σ_4 to negative values. The proposed method assigns $\sigma_4 = \sigma_4 - \sigma_3$ if $\sigma_3 < \sigma_4$ instead of assigning a negative value. The image A is divided into non-overlapping block B_k of size 4×4, singular value decomposition is applied to the block resulting in two orthogonal matrices U_k and V_k and a diagonal matrix S_k. The algorithm is presented in detail below.

Embedding Algorithm

Input: Block B_k, where $k = 0,1,2,3,\ldots,\frac{N \times N}{16} - 1$, binary secret message W, and its coordinate (i, j) generated by a random number generator seeded by a key K_1

Output: A stego image A'

Let $k = 0$.

Perform SVD on the block B_k, generating the corresponding U_k, S_k and V_k matrices. σ_p for $p = 1,2,3$ and 4 is the coefficient in S_k.

If $W(i, j) == 1$

$$\sigma_4 = \begin{cases} \sigma_2 - \sigma_3, & \text{if } \sigma_3 > (\sigma_2 - \sigma_3) \\ 0, & \text{otherwise.} \end{cases} \quad (5)$$

and $\sigma_2 = \sigma_2 + T$ such that a new diagonal matrix WS_k is obtained, where T is a threshold.

If $\sigma_3 < \sigma_4$, $\sigma_3 = \sigma_4$.

Perform inverse SVD on U_k, WS_k and V_k to reconstruct the stego block $WB_k = U_k WS_k V_k^T$

Let $k = k + 1$. Go to Step 2 until all binary pixels of the secret message have been embedded into the cover image.

Combine all stego blocks WB_k to form the stego image A'.

Extracting Algorithm

Input: Stego block WB_k, where $k = 0,1,2,3,\ldots,\frac{N\times N}{16} - 1$, and the coordinate (i,j) of extracted hidden message generated by a random number generator seeded by a key K_1.

Output: The extracted hidden message EW
Let $k = 0$.
Perform SVD on the block WB_k generating the corresponding UW_k, SW_k and VW_k matrices.

Let $SW_k = \begin{bmatrix} \sigma w_1 & 0 & 0 & 0 \\ 0 & \sigma w_2 & 0 & 0 \\ 0 & 0 & \sigma w_3 & 0 \\ 0 & 0 & 0 & \sigma w_4 \end{bmatrix}_j$

where $\sigma w_1, \sigma_{w2}, \sigma w_3$ and σw_4 are singular values of the block WB_k.
The extracted hidden message is given by

$$EW(i,j) = \begin{cases} 1, & \text{if } \sigma w_2 - \sigma w_3 > T/2. \\ 0, & \text{Otherwise.} \end{cases} \quad (6)$$

Let $k = k + 1$ and go to Step 2 until all hidden message bits are extracted.
Combine all stego blocks WB_k to form the extracted message.

5. EXPERIMENTAL RESULTS

The performance of SVD steganographic technique is evaluated in terms of normalized correlation (NC) and peak-signal-to-noise-ratio (PSNR). NC is used to evaluate the similarity between the original watermark and the revealed watermark and PSNR in dB is used to evaluate the similarity of the original image and the stego-image.

$$NC = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}\overline{W(i,j)\oplus W'(i,j)}}{N_1 N_2} \times 100\% \quad (7)$$

where $N_1 \times N_2$ is the size secret message, $W(i,j)$ and $W'(i,j)$ are the secret message bits and revealed secret message bit respectively at the location (i,j).

$$PSNR = 10log_{10}\frac{I_{max}^2}{MSE} \quad (8)$$

where I_{max} is the maximum of the three components of all the vector pixels over the original image and the MSE represents the mean square error between the stego-image and the original image. The MSE is given by

$$MSE = \frac{1}{MNC}\sum_{m=1}^{M}\sum_{n=1}^{N}|\boldsymbol{x}(m,n) - \hat{\boldsymbol{x}}(m,n)|^2 \quad (9)$$

where $M \times N$ is the size of the image, C is the number of channels of the image and $\boldsymbol{x}(m,n)$ and $\hat{\boldsymbol{x}}(m,n)$ are the original and output vector pixels respectively at the location (m,n).

Different colour images of such as Lena, Pepper, Kodak, Tiffany, House, Splash,

Tulips, Terrain, Airplane and Boat respectively of 512×512 size were used in experimentation. Representative of all images are shown in Figure 1 from (a) to (j). Original images are shown in Appendix C. The secret image to be hidden is shown in Figure 1 (k).

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k)

Figure 1. Representative images and watermark: (a) Lena, (b) Pepper, (c) Kodak, (d) Tiffany, (e) House, (f) Splash, (g) Tulips, (h) Terrain, (i) Airplane, (j) Boat and (k) Secret image.

Different types of attacks were used to test the robustness of the proposed steganographic method (PM). These tests are: Compression attack, Cropping attack, Impulse noise attack, Gaussian noise attack and Gamma correction attack.

The proposed method was compared with following different types of contemporary methods. Bergman's method (BM), proposed by Bergman and Davidson [C. Bergman et al., January 2005],Chang's method (CM), proposed by Chang et al [C-C. Chang et al., 2007] and Yang's method (YM), proposed by Yang et al [K-L., 2007].The following Table 1., Table 2., Table 3., Table 4., and Table 5. shows the results show the results of comparing the proposed method with BM, YM and CM for various attacks using Lena image.

Table 1. *Estimating secret message from Lena image for compression attack*

Quality of compression	BM		YM		CM		PM	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
50	49.73	31.96	32.86	34.05	75.26	32.02	76.12	32.02
60	50.58	32.21	33.44	34.53	85.76	31.80	85.88	31.80
70	51.14	32.54	35.91	35.14	97.29	31.48	97.24	31.46
80	53.68	32.95	43.21	35.98	99.80	31.65	99.92	31.65
90	54.51	33.58	64.20	37.70	99.95	32.66	99.92	32.67

Table 2. *Estimating secret message from Lena image for cropping attack*

% cropping ratio	BM		YM		CM		PM	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
10	66.33	14.88	90.96	14.91	91.74	15.00	92.04	15.00
20	67.77	11.94	84.91	11.95	85.18	12.62	85.62	12.62
30	67.40	9.99	78.73	9.99	78.46	11.10	78.90	11.10
40	68.26	8.72	70.82	8.72	71.85	10.02	71.89	10.02
50	68.72	7.85	63.62	7.86	65.35	8.90	65.21	8.90

Table 3. *Estimating secret message from Lena image for impulse noise attack*

Impulse noise ratio	BM		YM		CM		PM	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
0.05	58.66	23.01	76.36	23.27	74.85	23.08	75.87	23.02
.10	53.29	20.27	63.40	20.31	65.62	20.16	67.96	20.22
.15	49.78	18.48	57.69	18.59	63.86	18.50	63.89	18.53
.20	50.97	17.31	54.46	17.34	62.13	17.29	64.62	17.26
.25	47.50	16.33	51.19	16.37	62.74	16.33	62.71	16.35

Table 4. *Estimating secret message from Lena image for Gaussian noise attack*

Variance	BM		YM		CM		PM	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
.01	50.65	24.41	59.22	24.70	80.34	24.31	80.20	24.29
.02	49.58	21.67	56.00	21.81	69.11	21.64	68.84	21.61
.03	50.90	20.11	56.20	20.19	65.08	20.08	64.47	20.08
.04	49.95	19.01	54.73	19.09	63.35	19.02	62.23	19.00
.05	49.70	18.22	54.19	18.27	63.42	18.20	63.25	18.23

Table 5. *Estimating secret message from Lena image for Gamma correction attack*

Gamma	BM		YM		CM		PM	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
.8	67.28	26.44	31.81	26.73	99.58	26.35	99.97	26.33
.9	67.23	31.10	37.93	32.53	99.68	30.77	99.95	30.72
1.0	67.16	34.92	98.55	42.47	99.41	33.97	99.92	33.85
1.1	67.11	31.56	98.68	34.22	99.63	31.15	99.92	31.08
1.2	66.77	27.83	98.77	28.90	99.36	27.67	99.90	27.64

In Table 1. Quality of compression was taken from 50 to 90 in the increment of 10 for all results in these tables. Results of PM and CM were comparatively better than those of BM and YM for all qualities of compression under consideration in term of NC values for almost same PSNR values, with slightly better results for PM than CM. The Cropping ratios in Table 2. were taken from 10% to 50% in the increment of 10%. 10% cropping ratio is equivalent to removing 51 lines either from horizontal lines or vertical lines from the images of size 512×512. It was found that performance of PM is far better than that of BM and YM, and slightly better than that of CM in term of NC values for almost same values of PSNR. Table 3. show the results of comparing the proposed method with BM, YM and CM for impulse noise attack . Impulse noise ranging from 5% to 25% in the increment of 5% was injected to these images. It was found that performance of the proposed method is better than BM, YM and CM in term of NC values for almost same values of PSNR. Table 4. show the results of comparing the proposed method with BM, YM and CM for Gaussian noise attack . It was found that performance in descending order of various methods is CM, PM, YM and BM in term of NC values for almost same values of PSNR. Performance of CM and PM was neck to neck with slightly better result for CM.Table 5. show the results of comparing the proposed method with BM, YM and CM for Gamma correction attack using Lena image. It was found that PM outperformed other methods in term of NC values for these two images for Gamma values ranging from 0.8 to 1.2.

6. CONCLUSION

Many SVD based steganographic techniques were proposed in the literature by different authors. These SVD based steganographic techniques are robust to many different types of attacks such as Compression attack, Cropping attack, Impulse noise attack, Gaussian attack and Gamma correction attack .The proposed SVD based steganographic technique is quite robust to such attacks and more robust to other SVD steganographic techniques such as BM, YM and CM under consideration. It inserts the secret binary bits in singular values of SVD, keeping all singular values positive and in descending order of magnitudes unlike CM, in which singular values may be negative after inserting the secret bits. Secret bits are inserted to either left or right singular vectors in BM and YM, and robustness is less in such techniques. The future

plan of the proposed SVD steganographic technique is to develop a better one, which can withstand other different attacks including rotation attack, median filtering attack, scaling attack, blurring attack, sharpening attack, Stirmark attack etc.

7. REFERENCES

[1] C. Bergman and J. Davidson (January 2005), Unitary embedding for data hiding with the SVD, *Security, Steganography and Watermarking of Multimedia Contents VII, SPIE*, vol. 5681, San Jose CA.

[2] C-C. Chang , C-C. Lin and Y-S Hu (June 2007), An SVD oriented watermark embedding scheme with high qualities for the restored images, *IJICIC*, vol. 3, *no. 3*, pp. 609-620.

[3] C-H Hsu and C-C. Chen (May 2007), SVD based projection for face recognition, *IEEE EIT*, pp. 600-603.

[4] D.Q. Zhang , S.C. Chen and Z-H. Zhou (2005), A new face recognition method based on SVD perturbation for single example image per person, *Appl. Math Comp.*, vol. 163, *no.2*, pp. 895-907.

[5] E. Ganic and A.M. Eskicoglu (Sept. 2004), robust DWT-SVD domain image watermarking: Embedding data in all frequencies, *Proc. ACM Multimedia and Security Workshop*, pp. 166-171.

[6] H. Wang and S. Wang (October 2004), Cyber warfare Steganography vs Steganalysis, *ACM Commun*. vol. 47, pp. 76-82.

[7] J. Kaufman and M. Celenk (Oct. 2006), Digital video watermarking using singular value decomposition and 2D principal component analysis, *IEEE ICIP*, pp. 2561-2564.

[8] J-M. Shieh, D-C. Lou and M-C. Chang (April 2006), A semi blind digital watermarking scheme based on singular value decomposition, *Elsevier Computer Standards and Interfaces*, vol. 28, *issue 4*, pp. 428-440.

[9] K.B. Raja, S. Sindhu ,T.D Mahalakshmi, S. Akshatha ,B.K. Nithin ,M. Sarvajith, K.R Venugopal, I.M. Patnaik (6-10 January 2008), Robust image adaptive steganography using integer wavelets, *Proc. on 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE'*08, pp. 614-621,Bangalore.

[10] K.B. Raja, U. M. Rao , K.A. Rashmi , K.R Venugopal and U.M. Patnaik (20-22 December 2007), Robust and high capacity image steganography using SVD, *IET-UK ICTES*, pp. 718-723, Chennai.

[11] K.L. Chung, C-H. Shen and L-C. Chang (July 2001), A novel SVD- and VQ based image hiding scheme, *Elsevier Pattern Recognition Letters*, vol. 22, *Issue 9*, pp. 1051-1058.

[12] K-L. Chung, W-N Yang ,Y-H. Huang , S-T. Wu and Y-C. Hsu (May 2007), On SVD-based watermarking algorithm, *Elsevier Science Direct Applied Mathematics and Computation*, vol. 188, *no. 2007*, pp. 54-57.

[13] L. Hogben, R. Brualdi, A. Greenbaum and R. Mathias(2006), *Handbook of Linear Algebra*, Chapman & Hall/CRC.

[14] M.M. Hadhoud and A.A. Shaalan (14-16 December 2009), An efficient SVD image steganographic approach, *IEEE ICCES*, pp. 257-262, Cairo.

[15] M. S. Haghighi and S. Ghaemmaghami (2005), An optimal SVD-based watermarking framework through linear programming, *Proc. IASTED ICIMSA Euro IMSA 2005*, pp. 271-274.

[16] M. Sharif, S. Anis, M. Raza and S. Mohsin (2012), Enhance SVD based face recognition, *Journal of Applied Computer Science and Mathematics*, vol. 6,*no. 12*, pp. 49-53.

[17] R. A. Sadek (2008), Blind attack on SVD based watermarking techniques, *Proc. ACM CIMCA*, pp. 140-145.

[18] R Liu and T Tan (March 2002), An SVD watermarking scheme for protecting rightful ownership, *IEEE Trans. on Multimedia*, vol. 4, *no. 1*, pp. 121-128.

[19] V.I Gorodetski, L.J. Popyack, V. Samoilov and V.A. Skormin (2001), SVD-based approach to transparent embedding data into digital images, *Lecture Notes in Computer Science*, vol. 2052, pp. 263-274.

[20] X. Zhang and K. Li (2005), Comments on an SVD-based watermarking scheme for protecting rightful ownership, *IEEE Transaction on Multimedia*, vol. 7, *no. 3*, pp. 593-594.