Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.175 – 185

RESEARCH ARTICLE

Robustness Analysis of DWT-SVD with AES Encryption Based Highly Secure Image Data Hiding System via Various Attacks

Madhvi Dhankar[1], Jigyasha Soni[2]

[1]M.Tech Student, Rungta College of Engineering, Bhilai, Chhattisgarh, India

Email- madhvi.dhankar@gmail.com

[2]Assisstant Professor, Rungta College of Engineering, Bhilai, Chhattisgarh, India

Email- jigyasha.elex@gmail.com

Abstract: ***Unauthorized and illegal access of secure contents or data, along with manipulation of multimedia files over internet or wireless channels has been strongly noticed in the past few years. Lots of work is going on for the development of robust and efficient technique that can hide the secure data with high security and also have robustness against the various attacks often occurred after transmission of data in the wireless channels or internet. Most of the time a secure image which has to be transmit securely is first embedded on a cover image and the cover image will be then transmitted instead of original secure image. This process is known as invisible watermarking or also known as image data hiding. This is the most important and crucial process for transmitting a secure image over open communication channel. To effectively address this problem recently some hybrid transform techniques have gained attention due to their higher image data hiding efficiency. One of the most important candidates in this regard is DWT-SVD with AES encryption based image data hiding system [16].This paper present the robustness analysis of DWT-SVD with AES encryption based image data hiding system for various attacks. a novel technique for highly secure image data transmission based on discrete wavelet transform (DWT) and Singular value decomposition (SVD) based image data hiding along with advance encryption standard (AES) to enhance the security level. Particularly DWT and SVD based image data embedding over cover image is proposed to achieve higher robustness against various attacks, while AES ensures higher efficiency of transmission security. This hybrid technique leads to optimize both the fundamentally conflicting requirements. To present complete data security efficiency of the proposed technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed.***

Keywords: ***Image data security, attack robustness, image embedding, DWT, SVD, AES, PSNR, MSE, ER, BER***.

I. INTRODUCTION

In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Especially the case is more critical in the sense of image and video content privacy. Therefore a need for a robust method in order to protect the copy rights of media especially images and videos has become an essential constraint during the communication of secure images and videos over open communication channel. Invisible Digital watermarking provides copyright protection of data by hiding the secure data inside a cover image or video. It is also 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. For image watermarking, 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 or cover image, while transform domain schemes embed data by modifying transform domain coefficients [1,2]. 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 [3,5]. This provide most robust algorithm for many common attacks [7]. This paper presents the robustness analysis of DWT-SVD with AES encryption based image data hiding system for various attacks. A novel technique for highly secure image data transmission based on discrete wavelet transform (DWT) and Singular value decomposition (SVD) based image data hiding along with advance encryption standard (AES) to enhance the security level. Particularly DWT and SVD based image data embedding over cover image is proposed to achieve higher robustness against various attacks, while AES ensures higher efficiency of transmission security. This hybrid technique leads to optimize both the fundamentally conflicting requirements. To present complete data security efficiency of the proposed technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed.

This paper is organized as follows. The section2 briefly define the DWT, SVD techniques for data embedding along with the formal introduction to the advance encryption standard (AES). Section3 briefly describes the proposed image data hiding technique. The robustness performance evaluation of the DWT-SVD with AES encryption based image data hiding system for various attacks is given in Section 4, finally section 5 gives the conclusive remark of this work.

II. FUNDAMENTALS OF DWT, SVD AND AES

A. *Discrete Wavelet Transform (DWT)*

Wavelets are functions defined over a finite interval and have an average value equal to zero. The wavelet transform represents any arbitrary function (t) as a superposition of a set of basis function. These basis functions or baby wavelets are obtained from a single prototype wavelet called the mother wavelet. Basis functions include scaling function and wavelet function. The image is first divided into blocks and each block is then passed through the two filters: scaling filter (basically a low pass filter) and wavelet filter (basically a high pass filter). Four sub images are formed after doing the first level of decomposition namely LL, LH, HL, and HH coefficients [8-10].

At level 1: Image is decomposed into four sub bands: LL, LH, HL, and HH where LL denotes the coarse level coefficient which is the low frequency part of the image. LH, HL, and HH denote the finest scale wavelet coefficient. The LL sub band can be decomposed further to obtain higher level of decomposition. This decomposition can continues until the desired level of decomposition is achieved for the application. The secure image can also be embedded in the remaining three sub bands to maintain the quality of image as the LL sub band is more sensitive to human eye.

B. Singular Value Decomposition (SVD)

An image can be represented as a matrix of positive scalar values. Formally, SVD for any image say A of size $m \times m$ is a factorization of the form given by $A = U * S * V^T$, Where U and V are orthogonal matrices in which columns of U are left singular vectors and columns of V are right singular vectors of image A. S is a diagonal matrix of singular values in decreasing order. The basic idea behind SVD technique of watermarking is to find SVD of image and the altering the singular value to embed the watermark. In Digital watermarking schemes, SVD is used due to its main properties:

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

2) The singular value represents intrinsic algebraic image properties [4].

C. Advance Encryption Standard (AES)

The AES algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the key length can be 128, 192, or 256 bits, respectively. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total number of rounds is 10, 12, or 14, when the key length is 128, 192, or 256 bits, respectively. The 128-bit data block is divided into 16 bytes. These bytes are mapped to a 4×4 array called the State, and all the internal operations of the AES algorithm are performed on the State. Each round in AES, except the final round, consists of four transformations: Sub-Bytes, Shift-Rows, Mix- Columns, and Add-Round-Key. The final round does not have the Mix-Columns transformation. The decryption flow is simply the reverse of the encryption flow and each operation is the inverse of the corresponding one in the encryption process [11].

The initial step of AES is to convert the input plaintext matrix into state matrix. State matrix is obtained calculating hexadecimal value of input matrix which is given as input to the forthcoming steps of encryption. The plaintext matrix is rearranged into state matrix and iteratively loops the state through 4 steps: Addroundkey, Subbytes, Shiftrows, and Mixcolumns. The Addroundkey block performs bitwise xor of the state matrix and the round key matrix. The Subbytes block applies the S-box to one or more input bytes of input matrix. It performs the substitution function in which each byte of input matrix is replaced by the corresponding value in Sbox. The block shiftrows cyclically permutes (shifts) the rows of state matrix to the left. It takes the output matrix from subbytes step, cyclically shift the rows and give its output to next step. Polynomial matrices are used in the mixcolumns function, both matrices have the size of 4 × 4 and every row is a cyclic permutation (right shift) of the previous row. The mixcolumns transformation computes the new state matrix S0 by left multiplying the current state matrix S by the polynomial matrix P. The input parameters for encryption process are: the substitution table S-box, the key schedule w, and the polynomial matrix. The flowchart for AES encryption process is shown in Figure (1), figure (2) shows flow chart representation of AES decryption process.

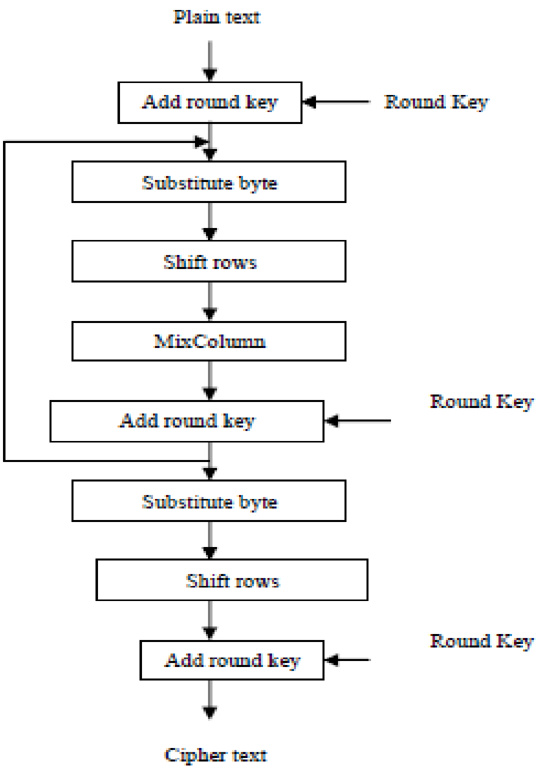


Figure (1). AES Encryption.

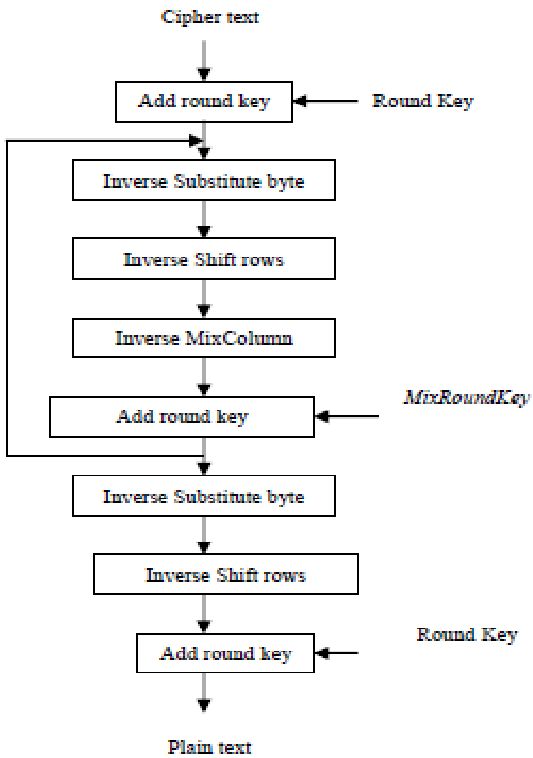


Figure (2). AES Decryption.

III. DWT-SVD BASED HIGHLY SECURE IMAGE DATA HIDING SYSTEM WITH AES ENCRYPTION

Any data hiding algorithm basically consists two sections, first one is the secure data hiding and next one is the extraction of secured data from the embedded cover image. This section briefly describes the DWT-SVD based image data hiding system with AES encryption technique [16].

A. DWT-SVD with AES Secure Image Data Embedding [16]

The main steps of DWT-SVD with AES secure image data embedding process are as follows:

1) Apply three level Haar DWT to decompose the cover or host image A in to four sub bands (i.e.,$L3$, $LH3$, $HL3$,$andHH3$).
2) Apply SVD to $HL3$ sub band of cover image i.e.,

$$A_C = U_C * S_C * V_C^T \quad \ldots(1)$$

Where $A_C = HL3$ sub band of cover image DWT decomposition.

3) Apply three level Haar DWT to decompose the secure image SI, (which isto be embed on the cover image) into four sub bands (i.e.,$L3$, $LH3$, $HL3$,$andHH3$).
4) Apply SVD to$HL3$ sub band of the secure image i.e.,

$$A_{SI} = U_{SI} * S_{SI} * V_{SI}^T \quad \ldots(2)$$

Where $A_{SI} = HL3$sub band of secure image DWT decomposition.

5) Modify the singular value of A_C by embedding singular value of A_{SI} such that

$$S_{CSI} = S_C + \alpha S_{SI} \quad \ldots(3)$$

Where S_{ISI} is modified singular matrix of A_C, and αdenotes the scaling factor which is used to control the strength of watermark signal

6) Next apply SVD to this modified singular matrix S_{ISI} i.e.,

$$S_{CSI} = U_{S_{CSI}} * S_{S_{CSI}} * V_{S_{CSI}}^T \quad \ldots(4)$$

7) Now obtain the modified DWT coefficients for cover image , i.e.,

$$A_{CSI} = U_C * S_{S_{CSI}} * V_C^T \quad \ldots(5)$$

8) Obtain the Embedded image A_E by applying inverse DWT using one modified A_{CSI} component and other non-modified DWT coefficients of cover image.
9) Now finally apply AES encryption to enhance security of this embedded image A_E .

B. DWT-SVD with AES Secure Image Data Extraction Process [16]

1) First apply AES decryption to obtain the embedded image A_E .
2) Apply three level Haar DWT to decompose the embedded image A_E in to four sub bands (i.e., $LL3$, $LH3$, $HL3$ and $HH3$).
3) Apply SVD to $HL3$ sub band i.e.,

$$A_{CSI} = U_{CSI} * S_{CSI} * V_{CSI}^T \quad \ldots(6)$$

Where $A_{CSI} = HL3$ of the decrypted and three level DWT decomposed embedded image A_E .

4) Compute $S_{SI}* = (S_{CSI} - S_C)/\alpha$, where $S_{SI}*$, is singular matrix of extracted Secured image.
5) Apply SVD to $S_{SI}*$ i.e.,

$$S_{SI}* = U_{S_{SI^*}} * S_{S_{SI^*}} * V_{S_{SI^*}}^T \quad \ldots(7)$$

6) Now Compute extracted secured image $SI*$ as,

$$SI* = U_{SI} * S_{S_{SI^*}} * V_{SI}^T \quad \ldots(8)$$

Finally the complete block diagram representation of the DWT-SVD with AES secure image data hiding and extraction systems are shown in figure (3) and figure (4).

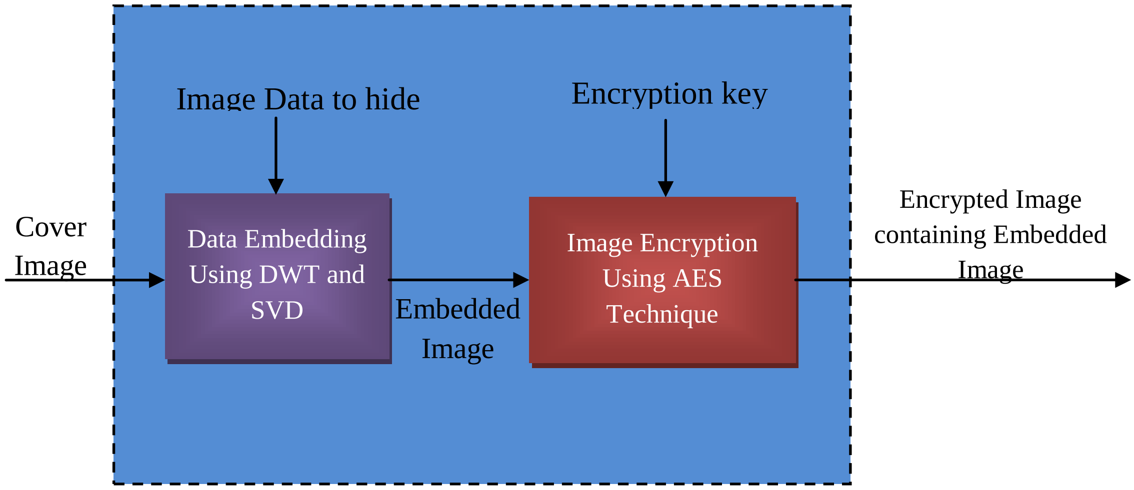


Figure (3) DWT-SVD with AES secure image data hiding system [16].

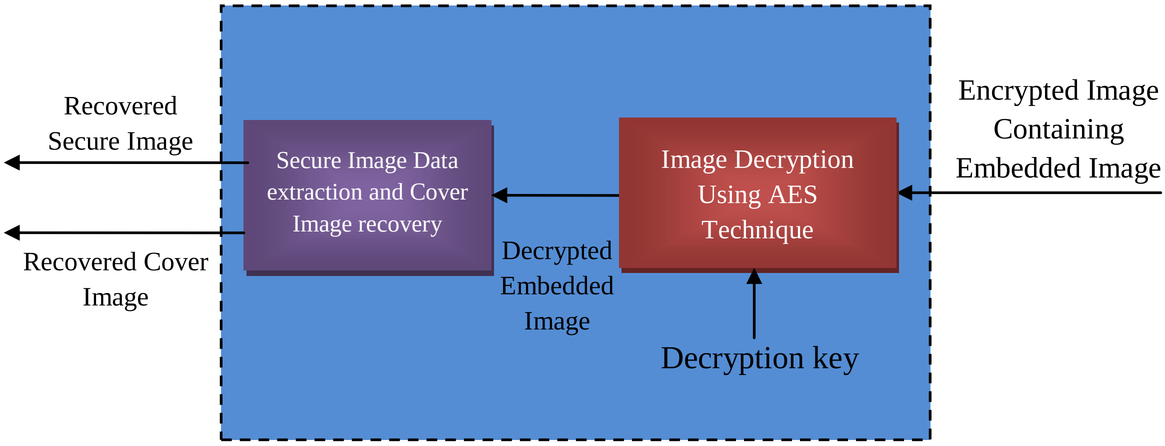


Figure (4) DWT-SVD with AES secure image data extraction system [16].

IV. ROBUSTNESS PERFORMANCE EVALUATION OF DWT-SVD BASED HIGHLY SECURE IMAGE DATA HIDING SYSTEM WITH AES ENCRYPTION

To demonstrate the robustness evaluation of DWT-SVD based highly secure image data hiding system with AES encryption, four different standard gray level image all of size 512 × 512 (Shown in Fig.5) have been used as the cover image and the gray level image "RCET.jpg" of size 64 × 64 (Shown in Fig.6)has been used as the secure image. For proper robustness evolution this system two important attacks have been considered, which are contrast attack and noise attack. To present complete data security efficiency of this technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed.

As discussed in previous section, the image data embedding capability of this system highly depends on the scaling factor α , hence in this paper, for robustness evaluation we will consider a constant value of scaling factor α , as $\alpha = 2$. The complete robustness evaluation of this system is divided in two parts : first part will present the robustness of this system against contrast variation of embedded image, while the second part will present its robustness against the white Gaussian noise variation.

(a) Lena.png (b) Barbara.png (c) Baboon.jpg (d) Peppers.jpg

Figure (5). Four standard test cover images used for performance evaluation.

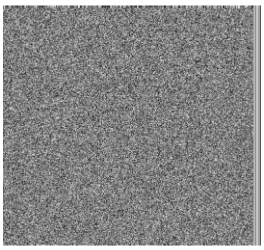
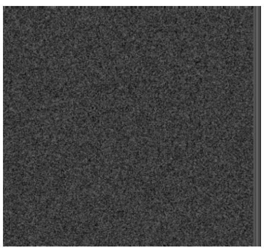
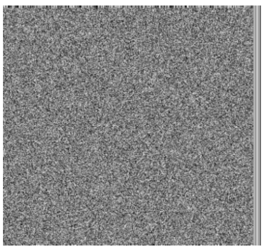
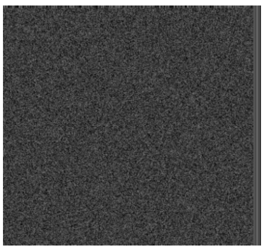
Figure (6). “Rungta.jpg” Used as Secure image.

A. *Robustness Evaluation of DWT-SVD Based Highly Secure Image Data Hiding System with AES Encryption for contrast variation*

This subsection presents robustness evaluation of DWT-SVD Based image data hiding system with AES encryption against the contrast variation of embedded image.

Consequently Table-1 shows the visual quality assessment of the DWT-SVD Based image data hiding system with AES encryption against the contrast variation, for this visual quality assessment “Lena.png” image has been considered as cover image. Table -2 shows the statistical performance parameters obtained after the robustness evaluation against contrast variation of the system with “Lena.png” as a cover image. On the same manner Table-3 to Table-5 gives the statistical performance parameters obtained after robustness evaluation against contrast variation of the system with “Barbara.png”, “Baboon.jpg” and “Peppers.jpg” as a cover image respectively.

Table 1. Robustness evaluation against contrast variation of the system with first test cover image “Lena.png”.

Contrast Reduction (in %)	AES Encrypted Embedded Image	Contrast Reduced AES Encrypt Embedded Image	Extracted Secure Image
10			
20			

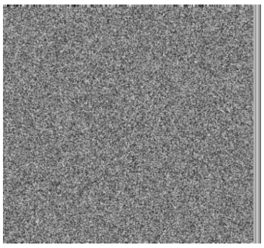
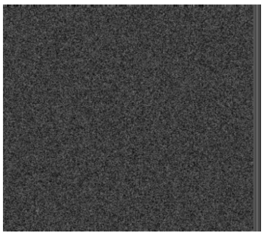
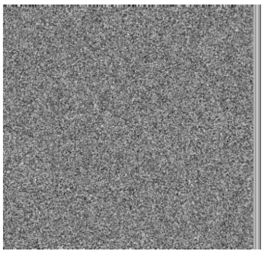
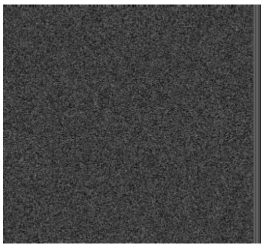
30			
40			

Table 2. Statistical Performance parameters obtained after Robustness evaluation against contrast variation of the system with first test cover image “Lena.png”.

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
10	Lena.jpg	Rungta.jpg	51.153	0.499	0.908	0.173
20			46.930	1.318	0.908	0.205
30			42.992	3.265	0.908	0.252
40			40.684	5.555	0.908	0.283

Table 3. Statistical Performance parameters obtained after Robustness evaluation against contrast variation of the system with second test cover image “Barbara.png”.

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
10	Barbara.png	Rungta.jpg	51.489	0.462	0.908	0.169
20			46.930	1.318	0.908	0.205
30			43.573	2.856	0.908	0.248
40			41.011	5.152	0.908	0.282

Table 4. Statistical Performance parameters obtained after Robustness evaluation against contrast variation of the system with third test cover image "Baboon.jpg".

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
10	Baboon.jpg	Rungta.jpg	53.181	0.313	0.908	0.160
20			47.787	1.082	0.908	0.206
30			44.640	2.234	0.908	0.242
40			42.276	3.850	0.908	0.283

Table 5, Statistical Performance parameters obtained after Robustness evaluation against contrast variation of the system with forth test cover image "Peppers.jpg".

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
10	Peppers.jpg	Rungta.jpg	50.650	0.560	0.908	0.187
20			45.808	1.707	0.908	0.229
30			42.596	3.577	0.908	0.265
40			40.418	5.905	0.908	0.304

From the visual inspection of the results obtained for robustness assessment of the DWT-SVD based image data hiding system with AES encryption against the contrast variation as shown in table-1, it is clearly observable that, the system provides a very good secure image quality even in the variation of contrast. This high quality secure image extraction capability is also subjectively reflected by table 2. Furthermore the same system has also been tested with three different test cover images against contrast variations. With the deep assessment of results obtained for other test images, the system is found efficient for image data hiding and quality extraction with all the test cover images against contrast variation.

B. Robustness evaluation of DWT-SVD Based Highly Secure Image Data Hiding System with AES Encryption for Noise variation

This subsection presents robustness evaluation of DWT-SVD Based image data hiding system with AES encryption against the noise variation in embedded image. For the noise addition in the embedded image white Gaussian noise have been employed.

Moreover Table-6 shows the visual quality assessment of the DWT-SVD Based image data hiding system with AES encryption against the white Gaussian noise variation, for this visual quality assessment here different test image "Baboon" has been considered as cover image. Table -7 shows the statistical performance parameters obtained after the robustness evaluation against contrast variation of the system with "Lena.png" as a cover image. On the same manner Table-8 to Table-9 gives the statistical performance parameters obtained after robustness evaluation against noise variation of the system with "Barbara.png", "Baboon.jpg" and "Peppers.jpg" as a cover image respectively.

Table 6. Robustness evaluation against contrast variation of the system with first test cover image "Baboon.jpg".

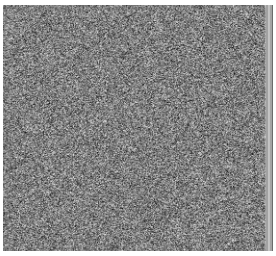
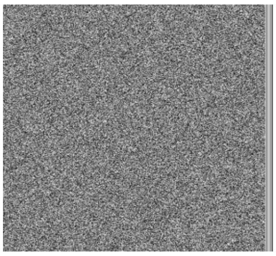
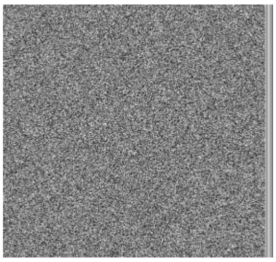
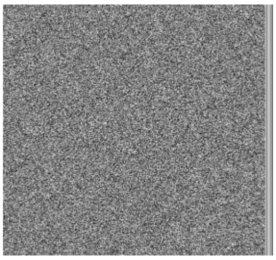
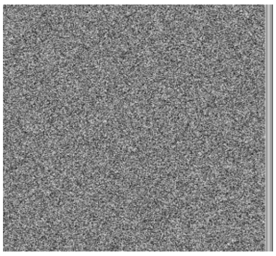
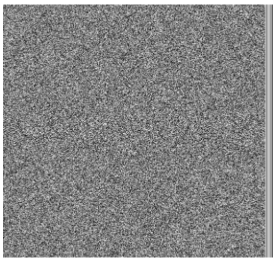
SNR Per sample	AES Encrypted Embedded Image	Contrast Reduced AES Encrypt Embedded Image	Extracted Secure Image
15			
20			
25			

Table 7. Statistical Performance parameters obtained after Robustness evaluation against noise variation of the system with first test cover image "Lena.png".

SNR Per Sample	**Cover Image**	**Secure Image (Rungta.jpg)**	**PSNR (in dB)**	**MSE**	**Embedding Rate (ER)**	**Bit-error Rate (BER)**
15	Lena.jpg	Rungta.jpg	40.350	5.999	0.908	0.838
20			48.639	0.890	0.908	0.466
25			55.107	0.201	0.908	0.226

Table 8. Statistical Performance parameters obtained after Robustness evaluation against noise variation of the system with second test cover image "Barbara.png".

SNR Per Sample	**Cover Image**	**Secure Image (Rungta.jpg)**	**PSNR (in dB)**	**MSE**	**Embedding Rate (ER)**	**Bit-error Rate (BER)**
15	Barbara.png	Rungta.jpg	42.486	3.668	0.908	0.774
20			49.007	0.817	0.908	0.500
25			55.765	0.172	0.908	0.217

Table 9. Statistical Performance parameters obtained after Robustness evaluation against noise variation of the system with third test cover image "Baboon.jpg".

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
15	Baboon.jpg	Rungta.jpg	40.663	5.582	0.908	0.784
20			48.563	0.905	0.908	0.509
25			56.181	0.157	0.908	0.173

Table 10, Statistical Performance parameters obtained after Robustness evaluation against noise variation of the system with forth test cover image "Peppers.jpg".

Contrast Reduction in Percentage	Cover Image	Secure Image (Rungta.jpg)	PSNR (in dB)	MSE	Embedding Rate (ER)	Bit-error Rate (BER)
15	Peppers.jpg	Rungta.jpg	41.821	4.275	0.908	0.835
20			49.987	0.652	0.908	0.438
25			55.038	0.204	0.908	0.219

From the visual inspection of the results obtained for robustness evaluation of the DWT-SVD based image data hiding system with AES encryption against the white Gaussian noise variation as shown in table-6, it is clearly observable that, the system again provides a very good secure image quality even in the presence of noise. This high quality secure image extraction capability is also subjectively reflected by table 7. Furthermore the same system has also been tested with three different test cover images. With the deep assessment of results obtained for other test images, the system is found efficient for image data hiding and quality extraction with all the test cover images in the noisy environment.

V. CONCLUSION

This paper put forwarded a complete robustness performance evaluation of DWT-SVD with AES encryption based image data hiding system for various attacks. The complete robustness evaluation of this system has been carried out with two different types of attacks that practically occurred in the transmission through the channel. The first attack considered is contrast attack, while the second one is the white Gaussian noise additions.

To present complete data security efficiency of the proposed technique various parameters like, peak signal to noise ratio (PSNR), mean square error (MSE), embedding rate (ER) and bit error rate (BER) have been employed.

From the visual inspection of the results obtained for robustness evaluation this system against the contrast variation and white Gaussian noise variation, it is clearly observable that, the system provides a very good secure image quality at the extraction side even in the presence of noise and variation in contrast. This high quality secure image extraction capability is also subjectively reflected by the tables given in the previous sections.

Furthermore the same system has also been tested with three different test cover images. With the deep assessment of results obtained for other test images, the system is also found robust for image data hiding and quality extraction with all the test cover images. Moreover it is also reflected from the tabulated values that, this system is capable to maintain the PSNR and MSE values for the good quality secure image extraction, and hence leads to a clear indication of the high robustness against the different attacks.

REFERENCES

[1] P. Ramana Reddy, Dr. Munaga.V .N. K.prasad, Dr. D. Sreenivasa Rao, ―Robust Digital Watermarking of Images using Wavelets.‖ International Journal of Computer and Electrical Engineering, Vol. 1, No. 2, June 2009.

[2] J. Sang and M. S. Alam, ―Fragility and robustness of binary-phase-only filter-based fragile/semifragile digital image watermarking,‖ IEEE Trans. Instrum. Meas., vol. 57, no. 3, pp. 595–606, Mar. 2008.

[3] R. Liu and T. Tan, ―An SVD-based watermarking scheme for protecting rightful ownership,‖ IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[4] H.-T. Wu and Y.-M. Cheung, ―Reversible watermarking by modulation and security enhancement,‖ IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 221–228, Jan. 2010.

[5] A. Nikolaidis and I. Pitas, ―Asymptotically optimal detection for additive watermarking in the DCT and DWT domains,‖ IEEE Trans. Image Process., vol. 12, no. 5, pp. 563–571, May 2003.

[6] V. Aslantas, L. A. Dog¢an, and S. Ozturk, ―DWT-SVD based image watermarking using particle swarm optimizer,‖ in Proc. IEEE Int. Conf. Multimedia Expo, Hannover, Germany, 2008, pp. 241–244.

[7] Chih-Chin Lai, and Cheng-Chih Tsai,‖ Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition,‖ IEEE Transactions on Instrumentation and Measurement., vol. 59, no. 11, pp. 3060-3063, Nov. 2010.

[8] Thakur, V. S., Thakur K. (2014). "Design and Implementation of a Highly Efficient Gray Image Compression Codec Using Fuzzy Based Soft Hybrid JPEG Standard". International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), pp.484,489, 9-11 Jan 2014.

[9] Thakur, V. S., Dewangan, N. K. and Thakur, K. (2014). "A Highly Efficient Gray Image Compression Codec Using Neuro Fuzzy Based Soft Hybrid JPEG Standard". Proceedings of Second International Conference, Emerging Research in Computing, Information, Communication and Applications (ERCICA), vol. 1, pp. 625-631, 9-11 Jan 2014.

[10] Thakur, V. S., Gupta, S. and Thakur, K. (2015). "Optimum Global Thresholding Based Variable Block Size DCT Coding For Efficient Image Compression". Biomedical & Pharmacology Journal, vol. 8(1), pp. 453-468, 2015.

[11] JebaNegaCheltha, C.; Velayutham, R , "A novel error-tolerant method in AES for satellite images" ,Emerging Trends in Electrical and Computer Technology (ICETECT), 2011.

[12] G. Bhatnagar and B. Raman, ―A new robust reference watermarking scheme based on DWT-SVD,‖Comput. Standards Interfaces, vol. 31, no. 5, pp. 1002–1013, Sep. 2009.

[13] E. Ganic and A. M. Eskicioglu, ―Robust DWT-SVD domain image watermarking: Embedding data in all frequencies,‖ in Proc. Workshop Multimedia Security, Magdeburg, Germany, 2004, pp. 166–174.

[14] Q. Li, C. Yuan, and Y.-Z. Zhong, ―Adaptive DWT-SVD domain image watermarking using human visual model,‖ in Proc. 9thInt. Conf. Adv. Commun. Technol., Gangwon-Do, South Korea, 2007, pp. 1947–1951.

[15] S. Mallat, ―The theory for multiresolution signal decomposition: The wavelet representation,‖ IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, pp. 654–693, Jul. 1989.

[16] Madhvi Dhankar and Jigyasha Soni "DWT-SVD Based Highly Secure Image Data Hiding System with AES Encryption" International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015.

