A Joint Encryption/Watermarking for Color Images

Smt.T Geetamma, J Beatrice Seventline

Abstract: ***With overwhelming use of internet, security is the top most priority while transferring data. This paper proposes a Joint encryption method along with Dual watermark embedding which gives ultimate security for multimedia file and also this procedure was implemented on color images.At first watermark is encoded with Chaotic mapping, after which it experience blended change inserting strategy dependent on DWT and DCT, with unique picture pursued by AES encryption for non-dazzle watermarking calculation. The DWT and DCT were joined to adapt to clamor issue and upgrade perceptual straightforwardness of watermarking picture. Our goal is to offer access to the results of the picture uprightness and of its inception despite the fact that the picture is put away encoded. This strategy gives better PSNR and relationship factors.***

Index Terms: AES, Toral automorphism, Joint Encryption, Dual watermarking.

I. INTRODUCTION

In the past several years there has been an explosive growth in digital imaging technology and applications. With this development Digital pictures and video are presently generally disseminated on the Internet and by means of CD-ROM. Computerized information, for example, advanced sound, pictures, and video, can be put away, replicated, and conveyed rapidly, effectively, and with no loss of loyalty. The achievement of the Internet, financially savvy and prevalent computerized recording and capacity gadgets, and the guarantee of higher data transfer capacity and nature of administration for both wired and remote systems have influenced it conceivable to make, to recreate, transmit, and disperse advanced substance in an easy way[14,15]. This regular utilization of the Internet has made a requirement for security. One issue with an advanced picture is that a boundless number of duplicates of a "unique" can be effectively conveyed or potentially manufactured. This presents issues if the picture is copyrighted. The assurance and requirement of licensed innovation rights has turned into a critical issue in the "computerized world[17,18]." As a result, to forestall data which has a place with legitimate proprietors from being deliberately or accidentally utilized by others, data insurance is imperative.

In the early days, encryption and control get to systems were utilized to secure the responsibility for.

Revised Manuscript Received on December 22, 2018.

Smt.T Geetamma, Department of ECE, GMR Institute of Technology,Rajam, India

J Beatrice Seventline,, Department of ECE, GITAM University, Vishakapatanm, Andhra Pradesh India.

In any case, to secure against unapproved duplicating after the media have been effectively transmitted and decoded, as of late the watermarking methods are used, in light of the fact that watermarking calculations insert the watermark into advanced information and the unapproved replicating can be counteracted by utilizing these watermark[16,17]. In this undertaking, a joint encryption and watermarking framework with blended change technique[1] is utilized for ensuring and checking the unwavering quality of pictures.

II. METHOD DESCRIPTION

System Architecture

The reason for our framework is to confirm the unwavering quality of the picture inside the unique space just as the encoded area. In this venture, the first shading picture is deteriorated into three parts Red, Green and Blue. The whole proposed method is connected for every Red, Green and Blue parts separately. The watermark is gone through the c-map for assurance of the first watermark through which the encryption procedure is done and afterward the watermark is put in the individual Red ,Green and Blue parts of shading picture to be transmitted. Presently these encoded watermarked pictures are took into consideration the watermarking pursued by the decoding which result the individual segments that can be transmitted. Thus the encryption and watermarking can be consolidated [2] which gives legitimization for the title joint encryption and watermarking which can be unmistakably clarified in underneath fig 1

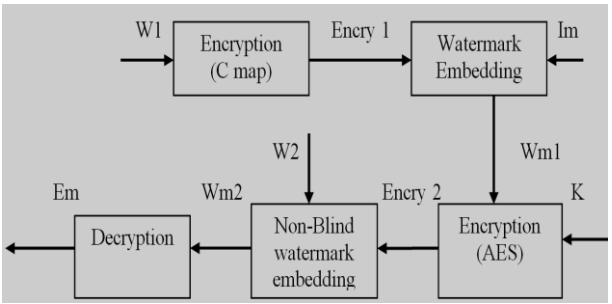

Fig. 1. System architecture

B. Embedding Algorithm Process:

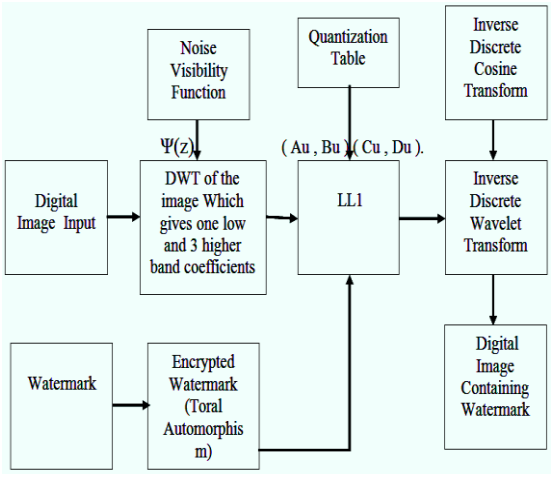

Fig. 2. Flow chart of embedded algorithm

C. AES encryption implementation:

This encryption method is implemented mainly using 4 steps which are shown as follows

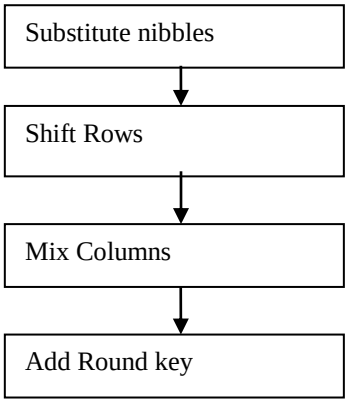

Fig. 3. AES encryption steps

Thus applying these steps on all color image components the encryption methods are carried out and thus the 3 images will get encrypted. These steps are followed based on the round around key given by the AES method.

Non Blind Watermark Embedding algorithm:

In this non-blind watermarking algorithm the actual image pixels are added by the watermark pixels by multiplying them with a constant factor say α.

The implementation can be given as

$$Wm = Im + (\alpha \times w)$$

Where Im is the original Image
α is the scaling factor
w is the watermark image.
Wm is the resulted watermarked image.

watermark detection process

The dual encrypted and watermarked images are taken /received and encrypted first then moves to the path for the detection of the watermark. Now the watermark detection process is applied to the encrypted images. The detected images are obtained when the non-blind watermarking is used and then watermark detected images are decrypted using the AES decryption method and thus at the last stage encryption and decryption is cleared[19,20]. Now the resulted images s de-watermarked using the blind watermarking technique which results the encrypted watermark. The process of this watermark detection is as shown in the following architecture.

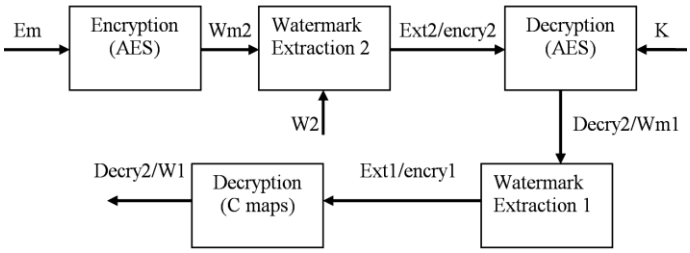

Fig.4. Watermark extraction process

D. Watermarking extraction scheme

The extracting stage utilizes the switch method as implanting stage. In the first place, it very well may be acquired from the highlights data of both unique picture and watermark . At that point, the scale and course of watermark picture will be altered with the information of highlight to make watermark and watermark picture synchronization.

The extraction of watermark with DWT and DCT will be under the condition of

If $(A_{z,u}, B_{z,u}) > (C_{z,u}, D_{z,u})$
V=black
Else
V=white

This means that if the coefficient value of z sub block coordinate $(A_u,B_u)$of DCT frequency domain is bigger than (C_u,D_u), then the pixel of watermark V will be black, otherwise ,it will be white.

E. AES decryption

This decryption method is implemented mainly using 4 steps which are shown as follows. Thus applying these steps on all 3 components of color image the decryption methods are carried out and thus the image will get encrypted. These steps are followed based on the round around key given by the AES method.

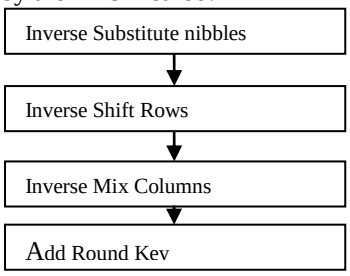

Fig.5. AES decryption steps

F. Non Blind Extraction algorithm:

In this non-blind extraction algorithm the embedded image pixels are subtracted by the watermark pixels by multiplying them with a constant factor say α.

The implementation can be given as

$$Im = Wm - (\alpha \times w)$$

G. Chaotic-map decryption:

The process of obtaining the original image using the transformed. Inverse Arnold Transform is obtained by using the equation below. Here $(x_1, y_1)^T$ is the coordinate of the Arnold transformed image pixel coordinates and $(x_1', y_1')^T$ is the original pixel coordinates.

$$\begin{pmatrix} X_1' \\ Y_1' \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ Y_1 \end{pmatrix} (\mathrm{mod}\, K)$$

Where K is the size of the image

III. RESULTS

Watermark embedding outputs

Fig.6. Input color image and Red, blue and green components separately

Fig.7. Input watermark image & Chaotic encryption output

Blind watermarking outputs

Fig.8. Blind watermarking output of Red, Green and Blue components

AES Encryption Outputs

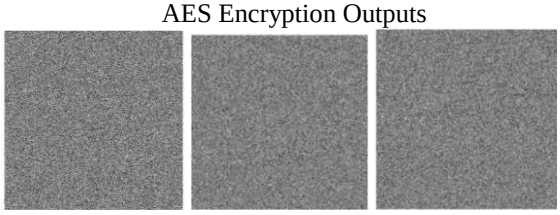

Fig 9. AES encrypted output of Red, Green & Blue

Non-blind watermarking outputs

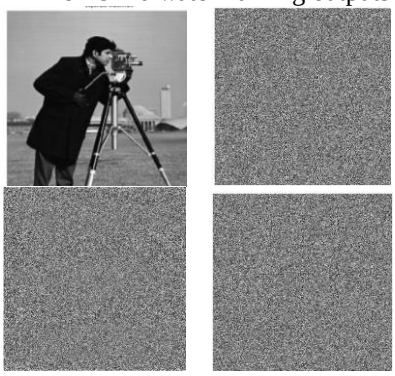

Fig.10.Non-blind watermark and RGB outputs of non-blind watermarking

Encrypted and Watermarked image

Fig.11. Encrypted and Watermarked image of Red ,Green & Blue component

Watermark detection outputs

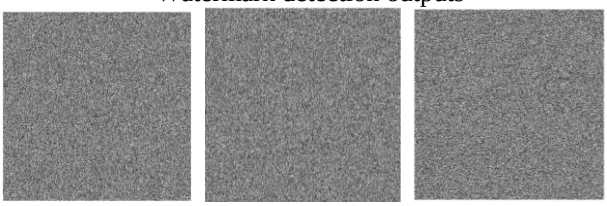

Fig.12.AES for embedded Red, Green & Blue Planes

Inverse AES encrypted image

Fig.13. Inverse AES of Red, Green & Blue component

Fig.14. Inverse blind watermarking output

Fig.15. watermark extracted

Table.1: PSNR and Correlation factors of RGB planes along with watermark

Parameters	Original & watermark encrypted red component	Original & watermark encrypted green component	Original & watermark encrypted blue component	Watermark
PSNR (dB)	37.6893	43.1444	44.8465	27.0927
Correlation coefficient	0.8778	0.8695	0.8393	0.67

IV .CONCLUSION

In this paper**,**another joint watermarking and encryption framework is proposed, which ensures from the earlier and a posteriori security of pictures. It blends a turbulent mapping, an encryption calculation which is a square figure calculation (e.g., AES) and substitutive visually impaired and non-daze watermarking calculations dependent on DWT and DCT. Trial results demonstrate that the picture mutilation is low and that the accomplished limit is sufficient to implant an unwavering quality verification just as some other data.Future works will concentrate on making our plan increasingly powerful to assaults like lossy picture pressure (e.g., JPEG) and lessening the multifaceted nature of our calculation. This scheme can be enhanced by combining with video watermarks. This project can also be extended by applying the scheme to specific environments or applications and examine its effectiveness.

REFERENCES

1. Chien-Pen Chuang , Cheng-Hung Liu , Yi-Tsai Liao , Huan-Wei Chi **"**A Robust Digital Watermarking with Mixed Transform Technique for Digital Image" – Proceedings of the International Multi Conference of Engineers and Computer scientists 2012 vol I IMECS 2012 march 14-16, Hong Kong.
2. Dalel Bouslimi, Member, IEEE, Gouenou Coatrieux, Member, IEEE, Michel Cozic,and Christian Roux, Fellow, IEEE "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images" IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 16, NO. 5, SEPTEMBER 2012.
3. Feng, l. and l. zheng and p. cao. "A DWT-DCT based blind watermarking algorithm for copyright protection**"** computer science and information technology (ICCSIT)**,** 3rd IEEE INTERNATIONAL CONFERENCE VOL. 7, PP. 455-458, 2010.
4. Li.X.S.Zheng ,Y.l. Zhao, H.M. Wu and S.F. Li, **"**Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform**,"** Proc. IEEE Symp. Electronic Commerce and Security, IEEE press, Aug.2008, pp.942-945,doi:10.1109 /ISECS .2008.140.
5. E.Chrysochos ,V.Fotopoulus M.Xenos **"**Chaotic-Correlation Based on Watermarking Scheme for Still Images" –Proceedings of "Applied Electronics 2008" Int. Conference, Pilsen, Czech Republic, 10-11 September 2008.
6. Elbasi and A. Eskicioglu, "A DWT-based robust semi-blind image watermarking algorithm using two bands," in Proc. IS&T/SPIE 18thAnnual Symp. Electronic Imaging, Security, Steganography, and Watermarking Multimedia Contents VIII Conf., San Jose, CA, Jan. 15–19,2006.
7. Zhao D., Guanrong C. and Wenbo L., "A Chaos based robust wavelet-domain watermarking algorithm", Chaos, Solitons and Fractals, vol. 22, pp. 47-54, 2004.
8. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proceedings of the IEEE, vol. 86, no. 6, pp. 1064–1087, 1998.
9. C. H. Lee and Y. K. Lee, "An adaptive digital image watermarking technique for copyright protection," IEEE Transactions on Consumer Electronics, vol. 45, issue. 4, pp. 1005–1015, Nov. 1999.
10. S. Voloshynovskiy , A. Herrigel , N. Baumgaertner and T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking," Proceedings of the Third International Workshop on Information Hiding, pp.211-236, Sep. 1999.
11. Voyatzis and I. Pitas, "Applications of Toral Automorphisms in Image Watermarking," In Proceeding of the IEEE InternationalConference on Image Processing, vol. 3, pp. 219-222, 1996.
12. Manoj.B, Manjula N Harihar , "Image Encryption and Decryption using AES" , International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012
13. Rafael C. Gonzalez , Richard E. Woods , " Digital Image Processing", second edition.
14. BalaAnand, M., Karthikeyan, N. & Karthik, S." Designing a Framework for Communal Software: Based on the Assessment Using Relation Modelling", Int J Parallel Prog (2018). https://doi.org/10.1007/s10766-018-0598-2
15. M.BalaAnand, S.Sankari, R.Sowmipriya, S.Sivaranjani "Identifying Fake User's in Social Networks Using Non Verbal Behavior", International Journal of Technology and Engineering System (IJTES), Vol.7(2), pg:157-161.
16. Maram, B., Gnanasekar, J.M., Manogaran, G. et al. SOCA (2018). https://doi.org/10.1007/s11761-018-0249-x
17. M. BalaAnand, N. Karthikeyan, S. Karthick and C. B. Sivaparthipan, "Demonetization: a Visual Exploration and Pattern Identification of People Opinion on Tweets," 2018 International Conference on Soft-computing and Network Security (ICSNS), Coimbatore, India, 2018, pp. 1-7. doi: 10.1109/ICSNS.2018.8573616
18. K. Anupriya, R. Gayathri, M. Balaanand and C. B. Sivaparthipan, "Eshopping Scam Identification using Machine Learning," 2018 International Conference on Soft-computing and Network Security (ICSNS), Coimbatore, India, 2018, pp. 1-7. doi: 10.1109/ICSNS.2018.8573687
19. CB Sivaparthipan, N Karthikeyan, S Karthik "Designing statistical assessment healthcare information system for diabetics analysis using big data" Multimedia Tools and Applications, 2018
20. Zemedkun Solomon, C.B. Sivaparthipan, P. Punitha, M. BalaAnand, N. Karthikeyan "Certain Investigation on Power Preservation in Sensor Networks" ," 2018 International Conference on Soft-computing and Network Security (ICSNS), Coimbatore, India, 2018, doi: 10.1109/ICSNS.2018.8573688