ENCRYPTED WATERMARK TECHNIQUES USING AES-128 IN DIGITAL PHOTOGRAPHY

Preeti Singh[1], Mukesh Tripathi[2]

[1, 2] *Electronics And Communicatio , RTU (India)*

ABSTRACT

Digital watermarking mainly used to transmit confidential data, by embedding that data into some color images. This paper presents a technique to implement data hiding in color images using Advanced Encryption Scheme (AES-128) and their restoration to original data to generate a time effective and secure technique. AES-128 is used to encrypt the data and to offer message authentication. Some tentative and structural designs are also given in this paper to explain the effectiveness of proposed technique.

Keywords: Digital Watermarking, Advanced Encryption Standard (AES-128), Structural Designs, And Data Hiding.

I. INTRODUCTION

Digital watermarking technologies allow users to embed digital code into images and video which are imperceptible during normal use but readable by computers and software. The additional information is called watermark. In the past few years, semi-fragile watermarking techniques have become increasingly important to secure and verify the multimedia content and also to localize the tampered areas. In digital photography, watermarking schemes are very important for copyright protection purposes. In this paper, Multimedia authentication and restoration system is projected with the defense of AES-128 ciphered and correlated watermarking. An encrypted image embedding is prepared by customized adaptation of Closest Point transform (CPT) in a digital photograph. A goal of this process is to diminish numerous security attacks. E.g. noise attack, compression attack, and cropping attack on multiple watermarked photographs and evaluated the proposed watermarking technique to examine the system robustness.

Existing System-

Existing watermarking techniques involve the concealment of information with a text or image and the transmission of this information to receiver with minimum distortion. This is a very new area of research. The technique will have a significant on defense, business, copyright protection and other fields where information needs to be protected at all costs from attacks. We just are embedding two images or test and images. Limitation of existing work counts very less security and more attacks. For the most part watermarks are utilized where confirmation or possession is required [1]. Watermarks are a decent route by which anybody can demonstrate that the sight and sound is identified with him. Additionally, watermark might be utilized to transmit secure message from one to other gathering, both fulfilling to utilize same method. Watermarks utilized ought to be

undetectable, as in, they are inserted into the picture in the wake of actualizing any cryptographic calculation. Being the need of more security, the confirmation can additionally be utilized. Validation could be given by utilizing Message Authentication Code, and installing this code into the picture as well. The issue comes here is the computational cost and time many-sided quality of utilizing a vigorous cryptographic calculation with some verification code calculation. Till now, the methods were utilizing the idea of message validation code just. Those methods were guaranteeing that if there comes any change in the message, it will be gotten as, when the validation code ascertained with the ruined message, it won't match the particular case that is in picture. Assume the situation when interloper not has any desire to change the message, in disdain he simply needs to take the message, such as replicating watchword. At this point, the past procedure falls flat, as the message is in plain content. Thus, a method ought to be proposed, which utilizes both message security, i.e., secrecy [2] and message validation i.e., honesty. This paper proposes such a procedure. At the point when advanced watermarking is utilized to transmit a mystery message, there are a few endeavors which are made by gatecrashers to perceive the mystery message. This is called as assault on picture being transmitted. The assaults may be classified in two classes, one is inactive assaults, in which the message substance is not adjusted, second is dynamic assaults in which the message substance is likewise altered.

There are several types of attacks being possible:

- Masquerading
- Fabrication
- Replaying
- Spoofing
- Denial of Service

Anyhow here the primary concern ought to be about how to secure the mystery data which is constantly transmitted by implanting into the picture. As now days, the more concern is of security with less time complex calculation to be use in encryption. On the off chance that any overwhelming calculation like RSA will be utilized, then the processing expense will rise to the sky, and if any low request calculation is utilized, the security will down beneath the earth. Consequently, a computationally cost and time powerful procedure ought to be executed, which ensures the security of message.

The remaining sections of the paper include:

Section 2: Literature review

Section 3: Proposed System Design

Section 4: Proposed Algorithm Approach

Section 5: Results

Section 5: Conclusion

II. LITERATURE REVIEW

The change received may be discrete cosine convert (DCT); discrete Fourier converts (DFT) and discrete wavelet changes (DWT) and so on. In the wake of applying change, watermark is implanted in the converted coefficients of the picture such that watermark is not unmistakable. At long last, the watermarked picture is gotten by procuring opposite conversion of the coefficients [3]. In peculiarity based watermarking plan, watermark is produced by applying a few operations on the pixel estimation of host picture instead of taking

from outer source. Late investigates on secure advanced watermarking methods have uncovered the way that the substance of the pictures could be utilized to enhance the imperceptibility and the power of a watermarking plan [4]. To enhance the security, Wang et.al [5] receive a key ward wavelet change. To exploit confinement and multi-determination property of the wavelet change, Wang and Lin [6] proposed wavelet tree based watermarking calculation. Tao et al. [7] set forward a discrete-wavelet converts based numerous watermarking calculations. The watermark is implanted into LL and HH subbands to enhance the heartiness. Luo et al. [8] presented a number wavelets based watermarking procedure to secure the copyright of computerized information by using encryption method to improve the security. Yuan et al. [9] proposed a number wavelet based multiple logos watermarking plan. The watermark is permuted utilizing Arnold change and is implanted by altering the coefficients of the HH and LL subbands. Qiwei et al. [10] set forward a DWT based visually impaired watermarking plan by scrambling the watermark utilizing disarray arrangement. A number of the calculations proposed meet the indistinctness prerequisite effectively yet vigor to diverse picture handling strike is the key test and the calculations in writing tended to just a subset of assaults.

III. PROPOSED SYSTEM DESIGN

Design is a creative process; a good design is the key to effective system. The system Design is defined as "The process of applying various techniques and principles for the purpose of defining a process or a system in sufficient detail to permit its physical realization". Various design features are followed to develop the system. The design specification describes the features of the system, the components or elements of the system and their appearance to end-users.

1. System Architecture

System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

The System architecture is shown below.

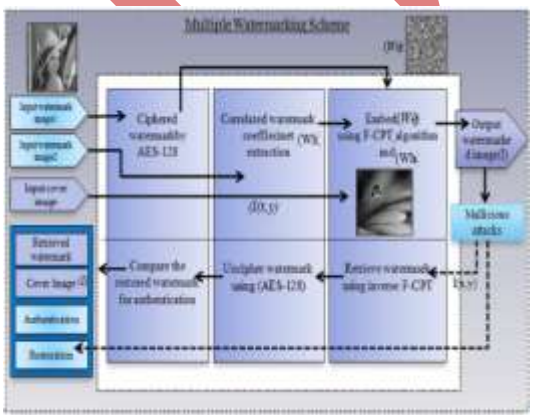


Fig. 1: System Architecture Of Proposed Solution

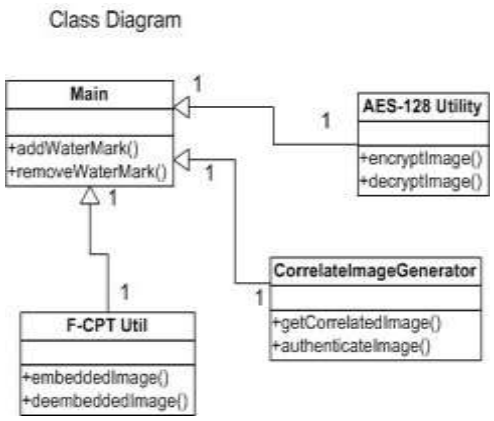


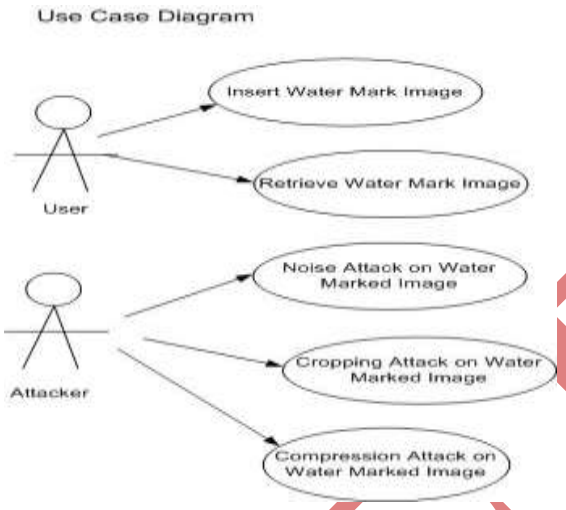
Fig. 2: Class Diagram Of Proposed Solution [7]

2. Classes Designed For The System

A class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes. The class diagram is shown by using Fig. 2.

3. Use Case Diagram Of The System

A use case diagram is a type of behavioral diagram created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.



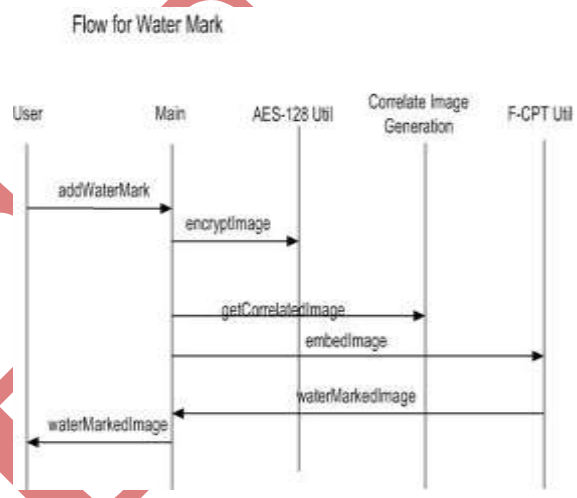
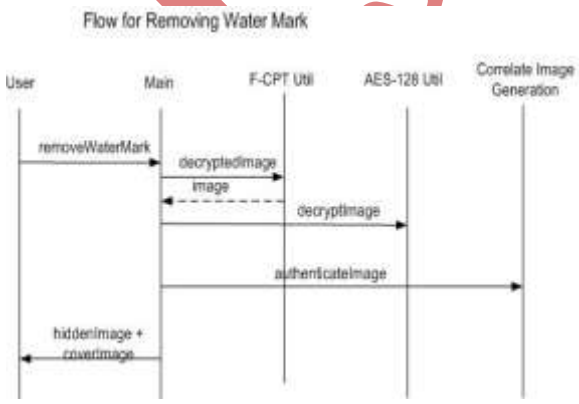


Fig. 3: Use Case diagram of proposed solution [8] **Fig. 4: Sequence flow diagram for watermarking [9]**

4. Sequence Diagram Of System Operation

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. The sequence diagrams shown below in Fig. 5



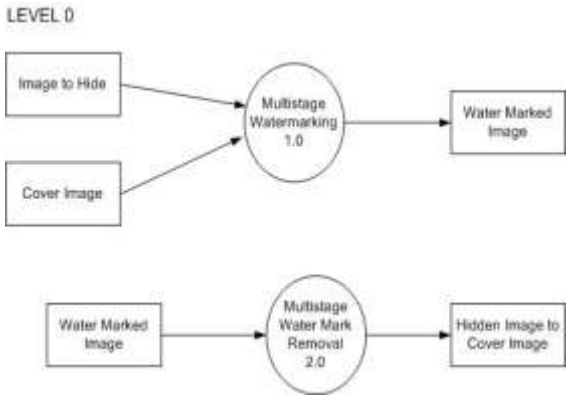


Fig. 5: Sequence flow diagram for removal of watermarking [9]

Fig. 6: Data flow diagram of level 0 of watermarking [11]

5. Data Flow Diagram Of The System

A data-flow diagram (DFD) is a graphical demonstration of the "flow" of data in the course of an information system. DFDs can as well be used for the visualization of data processing of any structured design. On a DFD, data items flow from an outer data source or an inner data store to an inside data store or an outside data sink, via an inner process.

5.1 Level 0 Data Flow Diagram

A context-level or level 0 data flow diagram shows the interface connecting the system and exterior agents which act as data sources and data sinks. On the framework graph (also known as the Level 0 DFD) the system's connections with the remote world are modeled simply in terms of data flows transversely the system limit. The framework plan shows the complete system as a particular process, and gives no clues as to its inner organization. [11]

5.2 Level 1 Data Flow Diagram

The Level 1 DFD shows how the system is divided into sub-systems (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system. [12]

Fig. 7: Data flow diagram of level 1 of watermarking [12]

IV. PROPOSED ALGORITHM APPROACH

Encrypted Watermark [13]

AES-128, key size=128

One round of AES consists of:

- Byte substitution
- Permutation
- Arithmetic operation
- XOR with generated key

Part image in 4 blocks of 128×128 bits

For block b=1:4

Permutation P = (Input (Arithmetic Operation) × XOR) / Byte substitution

Input (Row i=1, 2, 3,…..128) to AES-128

End

Encrypted watermark achieved

Authentication

- Retrieved watermark and embedded watermarks are compared
- Tampered locations are obtained where they are different

Restoration

- For image recovery we used the second watermark which is correlated watermark of the original image.
- This is called self-recovery process

V. RESULTS

Regardless of the fact that the sender breaks the encryption in the wake of accepting the picture from the owner, the perceptible and imperceptible watermarks will secure the responsibility for specific picture from the sender [14]. The fig 7 presents the watermarking process using encryption of two images and generating a third new image as output.

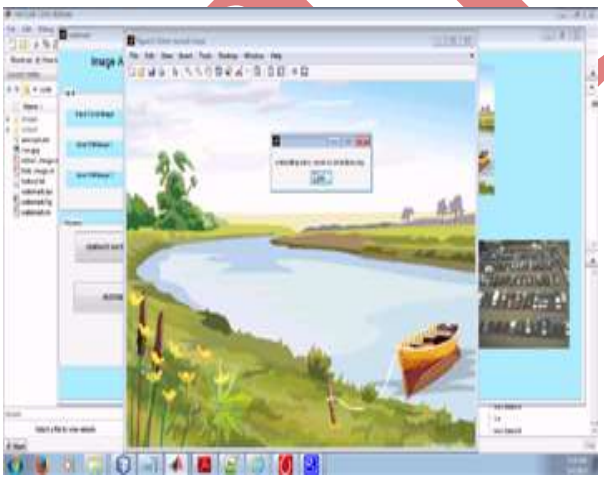


Fig. 7: Embedding Process Of Multiple Images Using Watermarking

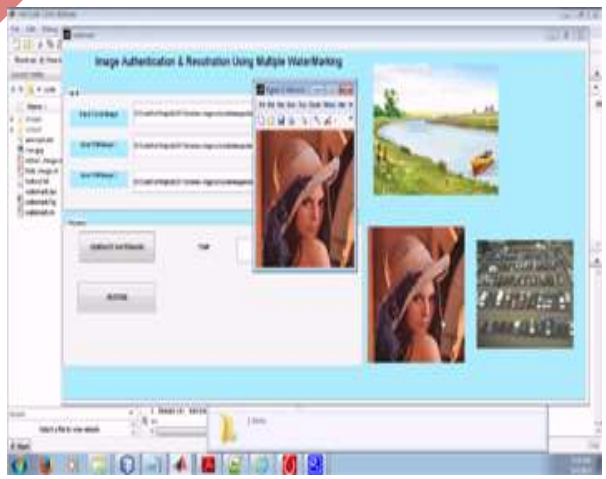


Fig. 8: Image Restoration

The Fig 8 shows the restoration process of Image 2 out of two encrypted images.

VI. CONCLUSIONS

In this paper, a multimedia authentication and restoration technique is proposed for digital photography. Security of AES-128 is used to make the ciphered watermark and embedded through modified F-CPT (feature closes point transform) for content authentication. Correlated watermark is embedded into wavelet sub-bands of cover image for content restoration. The results of proposed approach show that our system is highly robust and imperceptible.

NOMENCLATURE

b block (1:4)

P Permutation

AES Advanced Encryption Scheme (AES-128)

REFERENCES

[1] Ridzoň, R.; Levický, D.: Robust digital water marketing based on the log- polar mapping. In: Radioengineering. vol. 16, no. 4 (2007), p. 76-81.

[2] Ruanaidh, J.J.K., Pun, T.: "Rotation, scale and translation invariant digital image watermarking", in Proc. IEEE Int. Conf. Image Processing 1997, Santa Barbara, CA, vol. 1, pp. 536–539, Oct. 1997.

[3] T. D. Braun, H. J. Siegel, N. Beck, D. A. Hensgen, R. F. Freund, (2001) A comparison of eleven static heuristics for mapping a class of independent tasks on heterogeneous distributed systems, Journal of Parallel and Distributed Computing, ,pp.810- 837

[4] Q. Ying, and W. Ying, "A survey of wavelet-domain based digital image watermarking algorithm", Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

[5] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Trans. Image Process, 11, pp.77-88, 2002.

[6] S. H. Wang, and Y. P. Lin, "Wavelet Tree quantization for copyright protection for watermarking", IEEE Trans. Image Process, pp.154-165, 2002.

[7] P. Tao, and A. M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144, 2004.

[8] Y. Luo, L. Z. Cheng, B. Chen, and Y. Wu, "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005

[9] Yuan Yuan, Decai Huang, and Duanyang Liu, An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179, 2006.

[10] H. Dobbertin, V. Rtjimen, A Sowa Ed., "Advanced encryption standard-AES," ser. Leture Notes in Computer Science/Security and Cryptography, Bonn, Germany: Springer, 2004, vol. 3373.

[11] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[12] S. Changgui, B. Bharat, "An efficient MPEG videoencryption algorithm," Proc e edings of the symposium on reliable distributed systems, 2002, page(s):708,711.

[13] Y.-Y. Chen, H.-K. Pan, and Y.-C. Tseng, "A secure Data hiding scheme for two-color images," in Proc of 5th IEEE Symposium on computers and communications 2000, 2000, pp. 750-755.

[14] S: Riaz, K.H. Lee and S.-W. Lee, "Aesthetic Score Assessment based on Generic Features in Digital Photograph," 5th AUN/SEED Communication Technology, Manila, Philippine, Oct. 2012, pp.76-79.