ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Watermarking Techniques and Embedding Techniques using AES-128 in digital image and text files

Preeti Singh[1], Manju Mathur[2]

M.Tech, Digital Communication, RCEW, Jaipur, India[1]

Assistant Professor, Electronics, RCEW, Jaipur, India[2]

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.

Index Terms: Digital Watermarking, Advanced Encryption Standard (AES-128), Structural Designs, 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 this paper, Multimedia authentication and restoration system is projected with the defense of AES-128 ciphered and correlated watermarking. In a digital photograph to encrypt any image embedding it is prepared by customized adaptation of Closest Point transform (CPT). A goal of this process is to diminish numerous security attacks. E.g. cropping attack, compression attack and noise attack on numerous watermarked images and evaluated the recommended watermarking technique to study the strength of system.

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 innovative zone 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 algorithm. 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 algorithm with some verification code algorithm.

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

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

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 algorithm to be use in encryption. On the off chance that any overwhelming algorithm like RSA will be utilized, then the processing expense will rise to the sky, and if any low request algorithm 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 limitation and multi-determination property of the wavelet change, wavelet tree based watermarking algorithm is proposed by Wang and Lin [6]. Tao et al. [7] set forward a discrete-wavelet converts based numerous watermarking algorithms. The watermark is implemented into LL and HH sub-bands 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 logo watermarking plan. The watermark is permuted utilizing Arnold change. To implement watermark we could alter the coefficients of the LL and HH sub-bands. Qiwei et al. [10] set forward a DWT based visually impaired watermarking plan by scrambling the watermark utilizing disarray arrangement. A number of the algorithms proposed meet the indistinctness prerequisite effectively yet vigor to diverse picture handling strike is the key test and the algorithms 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 method of implementing numerous principles and techniques for the persistence of defining a significant process or a system to authorize its physical realization". Various design structures are surveyed to develop the system. The design specification describes the features of the system, the modules or elements of the system and their appearance to end-users.

A. System Architecture

System architecture is the conceptual design that defines the structure and behavior of a system. An design explanation is a prescribed description of a system, systematized in a way that supports perceptive about the fundamental properties of the system. It outlines the system modules or building blocks and delivers a plan from which products can be secured, and systems developed, that will work organized to implement the whole system.

The System architecture is shown below.

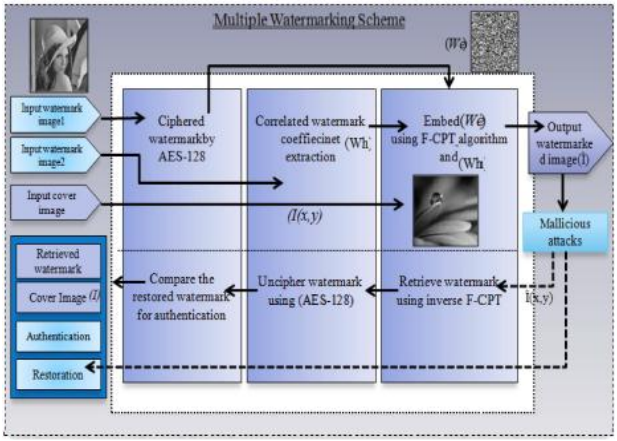

Fig. 1: System architecture of proposed solution

B. Classes Designed for the system

In the Unified Modeling Language (UML) atype of static structure diagram that is known as class diagram that defines the structure of a framework by presenting the elements of system's classes and the connections of classes with each other. The class diagram is shown below.

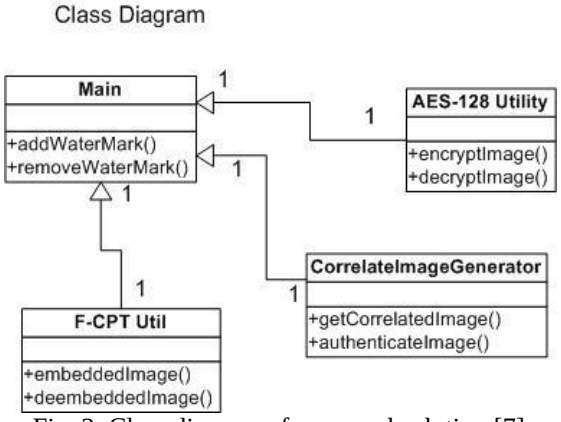

Fig. 2: Class diagram of proposed solution [7]

DOI 10.17148/IJARCCE.2015.41072

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

C. Use case Diagram of the system

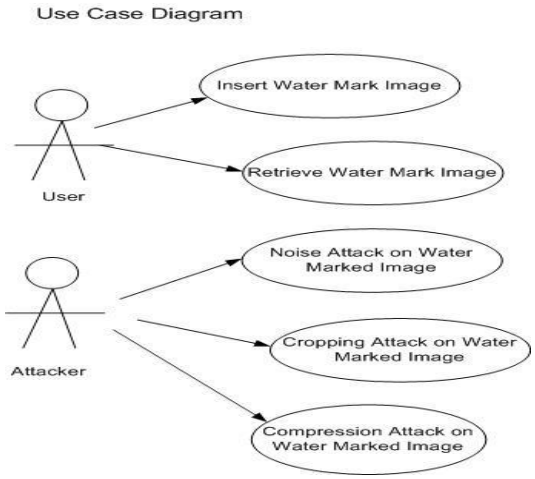

Fig. 3: Use Case diagram of proposed solution [8]

A use case diagram is a type of behavioral diagram created from a Use-case analysis. Its aim is to describe a graphical outline of the functionality provided by a system in terms of actors, their goals (denoted as use cases), and any dependencies among those use cases.

D. Sequence diagram of system operation

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes function with each-other and in what direction. It is a hypothesis of a Chart. The sequence diagrams shown below

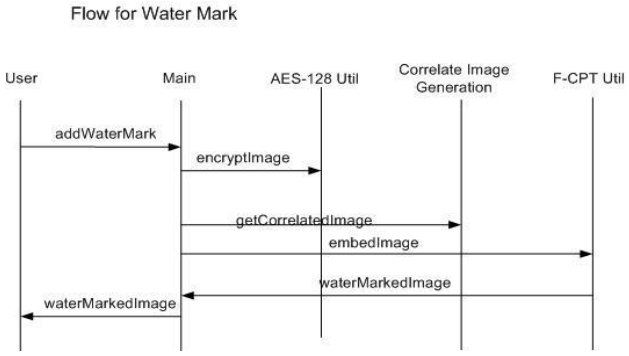

Fig. 4: Sequence flow diagram for watermarking [9]

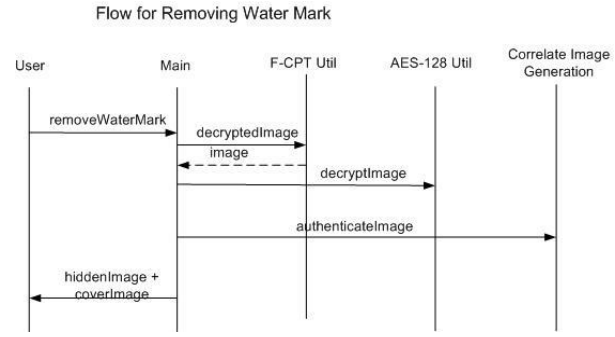

Fig. 5: Sequence flow diagram for removal of watermarking [9]

E. 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. In a DFD, flow of data items from an outer data source to an inner data source, via an inner process. DFDs can as well be used for the visualization of data processing of any structured design.

a) Level 0 Data flow diagram

A level 0 data flow diagram or context-level data flow diagram displays the exterior agents which act as data sources, interface connecting the system and data items and data links. On the structure graph the system's links with the remote world are exhibited simply in terms of data flows transversely the system limit. The framework plan shows the complete system as a particular procedure, and provides no indications as to its inner organization. [11]

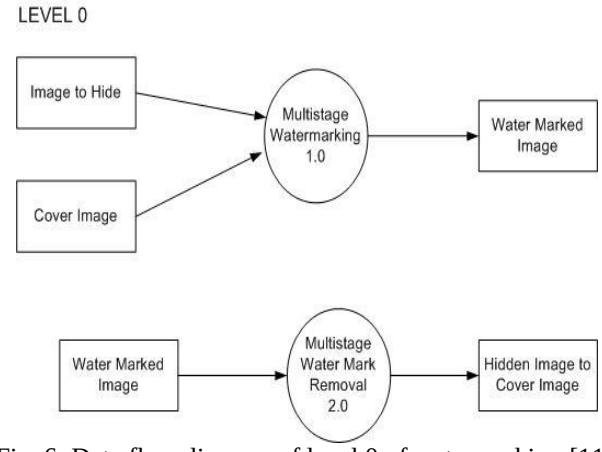

Fig. 6: Data flow diagram of level 0 of watermarking [11]

b) Level 1 Data flow diagram

The Level 1 DFD displays how the structure is distributed into sub-processes, every one of which deals with from an outer agent or one or more of the data flows, and which collectively deal all of the functionality of the scheme as a complete. It also classifies core data stores that essentials acceptable for the system to do its work, and shows the data flow concerning the numerous parts of the system. [12]

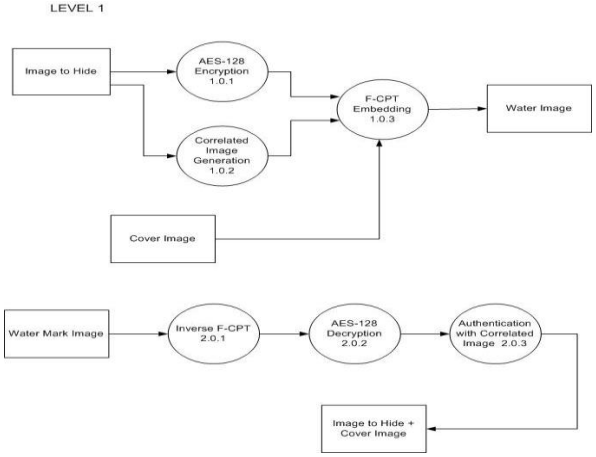

Fig. 7: Data flow diagram of level 1 of watermarking [12]

IV. PROPOSED ALGORITHM APPROACH

a) Encrypted Watermark [13]

AES-128, key size=128

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

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

- Recovered watermark and embedded watermarks are compared
- Tampered positions are found where they are diverse

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 2 presents the watermarking process using encryption of two images and generating a third new image as output.

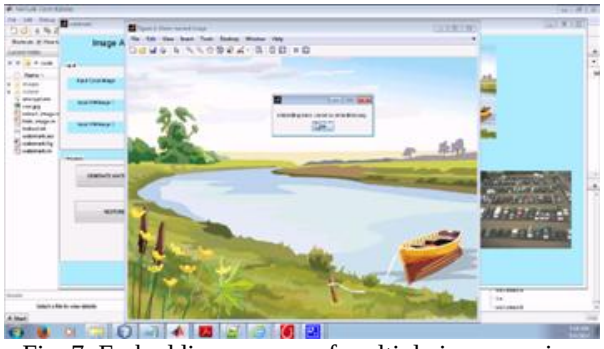

Fig. 7: Embedding process of multiple images using watermarking

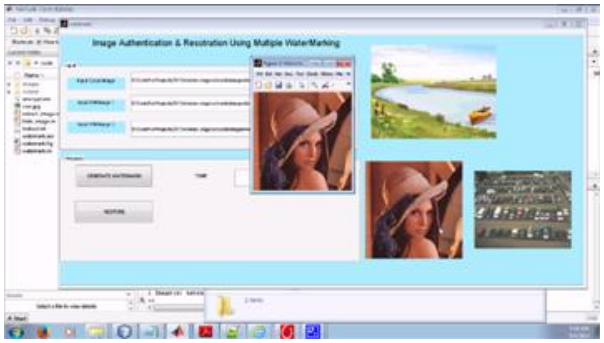

Fig. 8: Image restoration

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

VI. CONCLUSION

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.

ACKNOWLEDGEMENT

The authors convey their heartfelt thanks to **Mrs. Manju Mathur** (Assistant Professor), RCEW and **Mrs. Shweta Sharda**, (H.O.D, ECE Department), for providing them the required facilities to complete the project successfully. This paper is used to carry out a brief review about the digital watermarking techniques in image authentication and encryption.

REFERENCES

[1] Ridzoň, R.; Levický, D.(2007)"Robust digital water marketing based on the log- polar mapping". In: Radioengineering. vol. 16, no. 4, p. 76-81.
[2] Ruanaidh, J.J.K., Pun, T. (Oct. 1997) "Rotation, scale and translation invariant digital image watermarking", in Proc. IEEE Int. Conf. Image Processing 1997, Santa Barbara, CA, vol. 1, pp. 536–539.
[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, (2004) "A survey of wavelet-domain based digital image watermarking algorithm", Computer Engineering and Applications, Vol.11, pp.46-49.
[5] Y.Wang, J.F.Doherty, and R.E.Van Dyck, (2002) "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Trans. Image Process, 11, pp.77-88.
[6] S.H.Wang, and Y.P.Lin, (2002) "Wavelet Tree quantization for copyright protection for watermarking", IEEE Trans. Image Process, pp.154-165.
[7] P.Tao, and A.M.Eskicioglu, (2004) "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144.
[8] Y.Luo, L.Z.Cheng, B.Chen, and Y.Wu, (2005) "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103.
[9] Yuan Yuan, Decai Huang, and Duanyang Liu. (2006)"An Integer Wavelet Based Multiple Logo-watermarking Scheme". In IEEE, Vol.2 pp.175-179.
[10] H. Dobbertin, V. Rtjimen, A Sowa Ed., (2004) "Advanced encryption standard-AES," Leture Notes in Computer Science/Security and Cryptography, Bonn, Germany: Springer, vol. 3373.
[11] M. V. Droogenbroech, R. Benedett, (2002) "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts forIntelligent Vision Systems.
[12] S. Changgui, B. Bharat, (2002) "An efficient MPEG video encryption algorithm," Proceedings of thesymposium on reliable distributed systems, page(s):708,711.
[13] Y.-Y. Chen, H.-K. Pan and Y.-C. Tseng, (2000) "A secure Data hiding scheme for two-color images," in Proc of 5th IEEE Symposium on computers and communications, pp. 750-755.
[14] S: Riaz, K.H. Lee and S.-W. Lee, (Oct. 2012) "Aesthetic Score Assessment based on Generic Features in Digital Photograph," 5th AUN/SEED Communication Technology, Manila, Philippine, pp.76-79.