Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
3(1), 2015, 53-57

ISSN 2347 – 7393

Original Research Article

A WATERMARKING AND ENCRYPTION BASED IMAGE SHARING SCHEME

Brindha.R and Balaji.G

Communication systems, Department of ECE
Sri Shakthi Institute of Engineering and Technology Coimbatore, India

Abstract: Security is an important issue in the field of communication. While transmitting data through a network there is a chance for the data or information to get by an unauthorized person. So it is essential to take counter measures to provide confidentiality to our data as well as to prevent the unwanted access. Water marking is processes that enable us to hide our data in a medium like image. The medium is known as cover object. The main objective of the proposed work is to perform watermarking and to recover the data with minimized error.

Index Terms—water mark, security, confidential

I. Introduction

A watermark is a identifiable image or pattern in paper that appears as a variety of shades of lightness/darkness when viewed by transmit light (or when view by reflect light, atop a dark environment), caused by thickness or breadth variation in the paper. Watermarks have been used on postage trample, money, and other government documents to depress counterfeit. There are two main ways of producing watermarks in paper; the dandy roll process, and the more complex cylinder mould process.

Watermarks vary greatly in their visibility; while some are obvious on casual scrutiny, others require some study to pick out. Various aids have been developed, such as watermark fluid that wets the paper without harmful it. Watermarks are often used as security features of banknotes, passports, postage stamps and other documents to prevent counterfeit.

A watermark is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trade name and locations, and decisive the quality of a sheet of paper. Encoding an identify code into digitized music, video, picture or other file is known as a digital watermark.

II. Related Work

The present watermarking scheme is fail to make a decision the correct possession of an image. The key problems are then identified,

For Correspondence:
brindharam11@gmail.com
Received on: March 2015
Accepted after revision: March 2015
Downloaded from: www.johronline.com

and some important requirements for a valid invisible watermark detection.

The digital watermarking has been proposed by the copy right protection of an data or image. This technique is mainly based on the encoding schemes**.** Usual secure watermark detection techniques are designed to convince a verifier whether or not a watermark is fixed without disclosing the watermark pattern so that an untrusted verifier cannot remove the watermark from the watermark protected copy In this paper, we propose a compressive sensing based privacy preserve watermark detection structure that leverages secure multiparty computation and the cloud.

It has been shown that many signal processing algorithms performed in the CS domain have very close performance as performed in the original domain .Using random matrix transformation for privacy preserving data-mining has also been proposed, which proposed a accidental projection data perturbation approach for privacy preserving joint data-mining. The proposed a secure image retrieval system through random projection and have proven that the proposed random outcrop domain multimedia retrieval system is secure under the Cipher copy Only Attack model (COA) and the semi-honest model.

Furthermore that CS transformation can achieve computationally secure encryption. These works indicate that signal processing or data-mining in the CS domain is feasible and is computationally secure under certain conditions. In our framework, the target image/multimedia data is possessed by the image holder only. A compressive sensing matrix is issued by a certificate authority (CA) server to the image holder. The image holder transforms the DCT coefficients of the image data to a compressive sensing domain before outsources it to the cloud. For secure watermark detection, the watermark is transformed to the same compressive sensing domain using a secure multiparty computation (MPC) protocol and then sent to the cloud. The cloud only has the data in the compressive sensing domain.

Without the compressive sensing matrix, the cloud cannot reveal the original multimedia data and the watermark pattern. The cloud will perform watermark detection in the compressive sensing domain. The image data in the compressive sensing domain can be stored in the cloud and reused for detection of watermark from many other watermark owners.

In continuation of earlier work, where the problem of joint information embedding and lossless compression (of the composite signal) was studied in the absence and in the presence of attacks, here we consider the additional ingredient of protecting the secrecy of the watermark against an unauthorized party, which has no access to a secret key shared by the legitimate parties. In other words, we study the problem of joint coding for three objectives: information embedding, compression, and encryption. Our main result is a coding theorem that provides a single-letter characterization of the best achievable tradeoffs among the following parameters: the distortion between the composite signal and the cover text, the distortion in reconstructing the watermark by the legitimate receiver, the compressibility of the composite signal (with and without the key), and the equivocation of the watermark, as well as its reconstructed version, given the composite signal. In the attack-free case, if the key is independent of the cover text, this coding theorem gives rise to a threefold separation principle that tells that asymptotically, for long block codes, no optimality is lost by first applying a rate-distortion code to the watermark source, then encrypting the compressed codeword, and finally, embedding it into the cover text using a previously proposed embedding scheme. In the more general case, however, this separation principle is no longer valid, as the key plays an additional role of side information used by the embedding unit.

III. Proposed Method

A. *Watermark embedding process*

In embedding process, the algorithm achieves image integrity and authentication by adding the watermark to the image as shown in figure 1 according to the following steps:

(i)Extract groups.
(ii)Determine R–S-Vector.
(iii)Compress R–S-Vector.
(iv)Calculate the MD5 hash value of the image.

(v)Add the MD5 value to the compressed R–S-Vector and patient ID to get a watermark.
(vi)Encrypt the watermark using AES and Key 1.
(vii)The watermark is embedded by modifying the image using the watermark and key2.

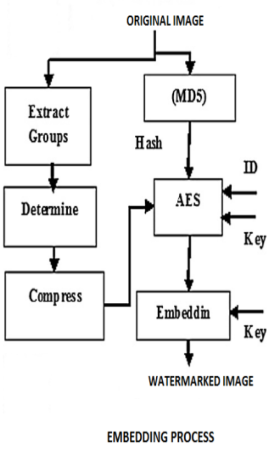

Fig.1Embedding process

A.Extract groups

In this step, the image is divided into groups; each group consists of four pixels, and it will be represented as a singular value. Discriminating and Flipping functions must be defined before identifying this single value of each group.

B. Flipping Function (F)

Flipping function is used to modify the pixel value by flipping the least significant bit. For example; if the value of a pixel before using this function equals 234 (that is represented in the binary system as 1110 1010). Then after using the function; the least significant bit will be flipped to be ‘‘1’’ instead of ‘‘0’’; accordingly, the value of this pixel will be 235 (that is represented in the binary system as 1110 1011).

The discrimination function is calculated for each group before (fBefore) and after (fAfter) using the flipping function; and the state of each group can be determined as follows

R Group (Regular group):
if f After > f Before
S Group (Singular group):
if f After < f Before
U Group (Unused group):
if f After= f Before

C. Watermark extracting process

In Extraction process, the original image is retrieved, and the watermark is extracted from the watermarked image. This process shown in figure 2 consists of the following steps:

1. Extract groups. (4 pixels per Group)
2. Determine The R–S-Vector and extract the encrypted watermark.
3. Decrypt the watermark using AES.
4. Extract the hash value (MD5), patient ID and the R–S-Vector of the original image.
5. Decompress the R–S-Vector.
6. Extract the original image (non-watermarked image).
7. Calculate the hash value (MD5) of the extracted original image.
8. Compare the calculated hash value (step5) and the extracted hashes value (step2), if they are equal, the image is authenticated, and it has right integrity, else the image is discarded because its integrity is broken. The flipping function is also defined.

Modifying the original image according to the watermark In this step, the watermark is embedded into the image; the state of each group of pixels of the original image is modified using the flipping function to represent one bit of the watermark; the output image of this step is called the watermarked image. It is optional to select the group of pixels randomly using key2 as a seed of the random number generator, this to distribute the watermark randomly inside the image.

Extract groups and Create R–S-Vector processes will be D one as in the embedding process. The encrypted watermark consists of the compressed R–S-Vector and the hash value (MD5) of the original image; identify the compressed R–S Vector and the hash value (MD5). The AES is used to decrypt the watermark using (key1).Then the decrypted R–S-Vector is decompressed using Extended Huffman algorithm. The original image is extracted

A proposed security technique based on watermarking and encryption for digital imaging 5 by modifying the groups’ status of the watermarked image to become identical to the decompressed R–S-Vector. The MD5 Hash value of extracted non-watermarked image is calculated; it is compared with the decrypted MD5 hash value, if they are equal, then the image is not modified, and it is validated, otherwise the two hash values are different, therefore, the image was modified, and it is no longer authenticated. If the image is authenticated, it is proven that its integrity is right and the encryption process is implemented with a legal user within the medical system because he has the private key, in addition the identity of the patient is identified using the extracted patient ID.

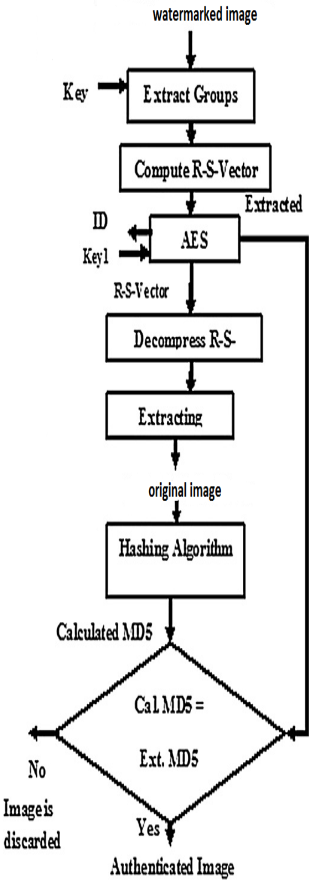

Fig.2 Extracting process

IV. Simulation

The simulation is done with the help of MATLAB which stands for Matrix Laboratory. Watermarking shown in figure 5 & figure 6 and encryption which is shown in figure 7 are done on secret image as in figure 3 and cover image as in figure 4. The secret image, cover image, watermarked image, encrypted image are shown.

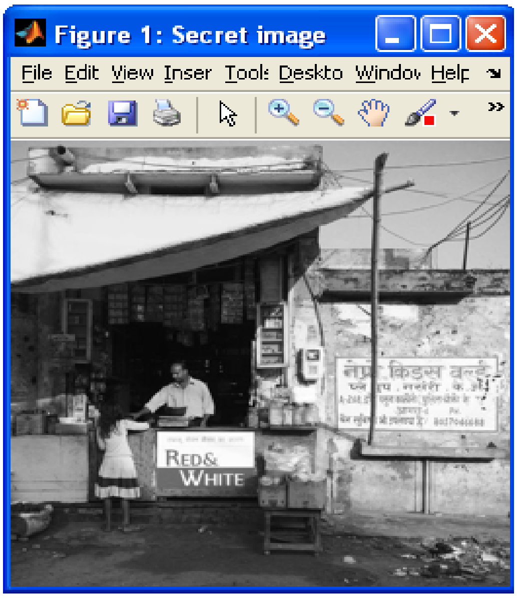

Fig 3. Secret image

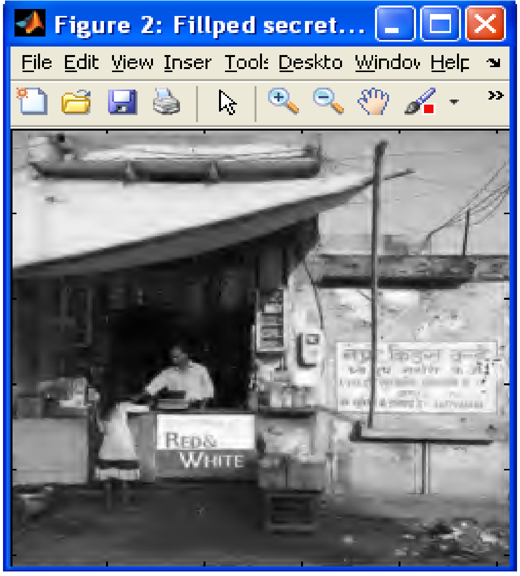
Figure 2: Fillped secret...
File Edit View Inser Tool: Deskto Windov Help

Fig 4. Fillped secret image

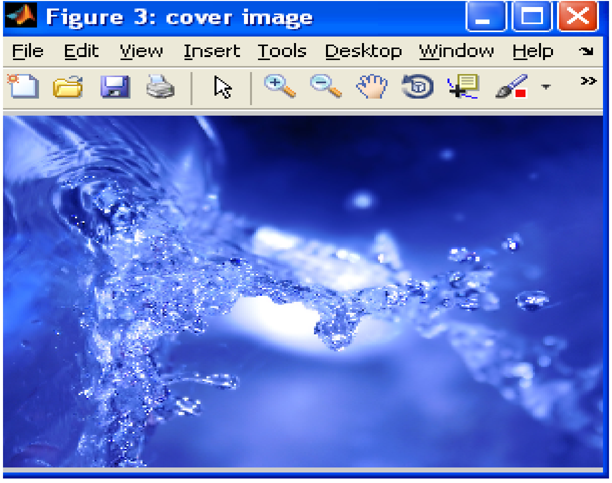

Fig. 5 Cover image

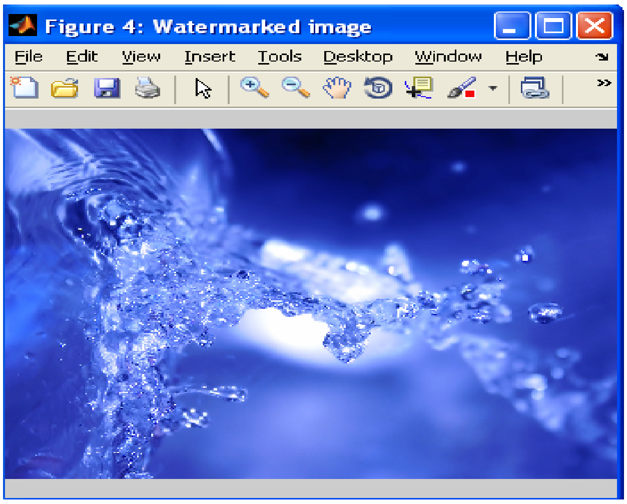
Figure 4: Watermarked image
File Edit View Insert Tools Desktop Window Help

Fig 6. Watermarked image

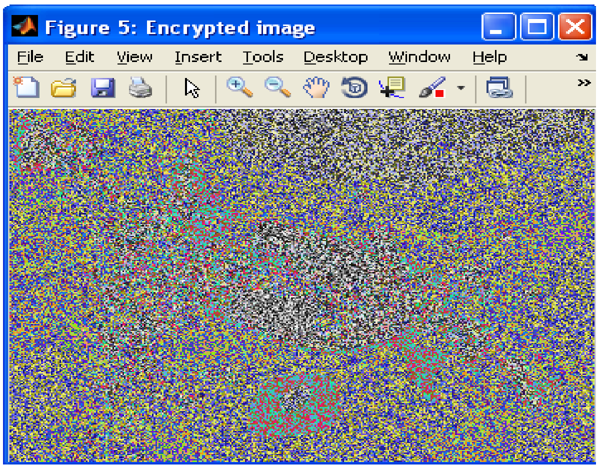
Figure 5: Encrypted image
File Edit View Insert Tools Desktop Window Help

Fig 7. Encrypted image

V. Conclusion

The watermarking and encryption of the watermarked and encrypted image is implemented using MATLAB. The SNR, PSNR, and MSE is calculated, to evaluate the accuracy of watermarking and encrypted image & its detection. The BER is found out to identify the matching between embedded image and retrieved image.

Acknowledgement

First of all we sincerely thank the almighty who is most beneficent and merciful for giving us knowledge and courage to complete the project work successfully. We also express our gratitude to all the teaching and non-teaching staff of the college especially to our department for their encouragement and help done during our work. Finally, we appreciate the patience and solid support of our parents and enthusiastic friends for their encouragement and moral support for this effort.

References

[1] Coatrieux G, Montagner J, Huang H, Roux C. Mixed reversible and RONI watermarking for digital image reliability protection. In: 29th International conference of the IEEE, engineering in medicine and biology society, Lyon, 2007. pp. 5653–6.

[2] Memon N, Gilani S. Adaptive data hiding scheme for digital images using integer wavelet transform. In: IEEE international conference on emerging technologies, Islamabad, Pakistan, 2009. pp. 221–4.

[3] Lim Y, Feng D. Multiple block based authentication watermarking for distribution of medical images. In: International symposium on intelligent multimedia, video and speech processing,

[4] Boucherkha S, Benmohamed M. A lossless watermarking based authentication system for medical images. Int J Signal Process 2004, vol.1, no.4, pp 278–81.

[5] Mostafa S, El- sheimy N, Tolba A, Abdelkader F, Elhindy H. Wavelet packets-based blind watermarking for digital image management. Open Biomed Eng J 2010; vol.4: pp 93–8.