International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(4), pp.014-018
DOI: http://dx.doi.org/10.21172/1.94.03
e-ISSN:2278-621X

IMPLEMENTATION OF LOSSLESS VISIBLE WATERMARKING AND DATA HIDING USING ADVANCED ENCRYPTION STANDARD ALGORITHM

Vinod Khetade[1]

Abstract-Digital watermarking's demand is on high for Copyright protection of intellectual properties due to advancements of computer technologies and the fast and increased use of the internet have made reproduction and distribution of digital information easier than ever before. In this paper, a method for visible watermarking with lossless image recovery using reversible compound mapping is proposed. The method uses one-to-one compound mappings that adjust the mapping to obtain pixel values close to those of the desired visible watermarks. The mappings are proved to be reversible for lossless recovery of the original image. The proposed system also includes implementation of security tool that hides data into the image in the form of text using AES algorithm.
Keywords – Digital watermark, Compound mapping, encryption, decryption data hiding.

1. INTRODUCTION

Information is increasingly important in our daily lives. We have become information dependents living in an on command, on demand world that means we need information everywhere and every time. We access the Internet every day to perform searches, participate in social networking such as Facebook twitter, send and receive e-mails, share pictures and videos. Most of the people have gadgets such as digital camera, smartphones, and laptops and using such content-generating devices, more information is being created by individuals than by businesses. Such development of sophisticated computer technologies and increased fast and affordable internet connections, the digital information can be easily shared processed or used causing serious security problems such as ownership identification, Illegal distribution and so on. One of the possible solutions is the digital watermarking.

Digital watermarking is digital logo, pattern or ownership descriptions embedded into the media for protecting intellectual property right. Digital watermarking techniques for images are of two types: visible and invisible. Visible watermark are generally clearly visible after common image operations are applied because it convey ownership information directly on the image and can deter attempts of copyright violations. The invisible watermark aims to embed copyright information imperceptibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to identify the ownership of the protected host. It is important that the watermark must embed well with the host image without much loss of original image details and survives any kind of image manipulations.

2. LITERATURE SURVEY

Today there is a numerous of techniques for image watermarking. The most common approach is to compress a portion of the original host image and then embed the compressed data together with the intended payload into the host [1], [2]. Second approach is to manipulate a group of pixels as a unit to embed a bit of information [3], [4]. As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region [5], [6], [7]. Another approach is to rotate consecutive watermark pixels to embed a visible watermark [7].Another approach for visible watermarking is using FPGA which provides one to one compound mapping that allows reversible watermarking [8]. Secure transmission of secrete file preventing any third party access and security level of data is increased by encrypting data using AES algorithm and lossy technique[10].

3. REVERSIBLE ONE-TO-ONE COMPOUND MAPPING

First, we propose a generic one-to-one compound mapping [9] for converting a set of numerical values,
$P = \{p1, p2....., p_M\}$ to another set $Q = \{q1, q2....,q_M\}$, that the respective mapping from p_i to q_i for all i = 1,2,.....,M is reversible. Here, for the copyright protection applications investigated in this study, all the values p_i and q_i are image pixel

[1] Department of Computer Science and Engineering, D.K.T.E's Textile and Engineering Institute, Ichalkaranji, Maharashtra, India

values (grayscale or color values). The compound mapping f is governed by a one-to-one function F_x with one parameter x = a or b in the following way:

$q = f(p) = F_b^{-1}(F_a(p))$ (1)

where F_x^{-1} is the inverse of F_x which, by one -to-one property , leads to the fact that if $F_a(p)= p'$, then $F_a^{-1}(p') = p$ for all values of a and p. On the other hand, $F_a(p)$ and $F_b(p)$generally are set to be unequal if a !=b. The compound mapping described by (1) is indeed reversible, that is , p can be derived exactly from using q the following formula:

$p= f^{-1}(q) = F_a^{-1}(F_b(q))$ (2)

The proposed generic lossless watermarking method is based one-to-one compound mappings that adjust the mapping to obtain pixel values close to those of the desired visible watermarks. The compound mappings are proved to be reversible, which allows for lossless recovery of original images from watermarked images. Visible watermarking scheme with a given image I and a watermark L as input is described as an algorithm [9] as follows:

Algorithm 1- Generic Visible Watermark Embedding

Input: an image I and a watermark L

Output: Watermarked image W

Steps:

1)Select a set P of pixels from I where L is to be embedded and call P a watermarking area.

2) Denote the set of pixels corresponding to P in W by Q.

3)For each pixel X with value p in P , denote the Corresponding pixel in Q as Z and the value of the corresponding pixel Y in L as l ,and conduct the following steps.

a) Apply an estimation technique to derive a to be a value close to p , using the values of the neighbouring pixels of X .

b) Set b to be the value l.

c) Map p to a new value $q= F_b^{-1}(F_a(p))$.

d) Set the value of Z to be q.

4) Set the value of each remaining pixel in W, Which is outside the region P , to be equal to That of the corresponding pixel in I .

Note that we do not use the information of the original image pixel value of X itself for com- putting the parameters a and b for X. This ensures that identical parameter values can be calculated by the receiver of a watermarked image for purpose of lossless image recovery.

Algorithm 2- Generic Watermark Removal for Lossless Image Recovery

Input: a watermarked image W and a watermark L

Output: the original image R recovered from W.

Steps:

1) Select the same watermarking area Q in W as that selected in Algorithm 1.
2) Set the value of each pixel in R, which is outside the region Q, to be equal to that of the corresponding pixel in W.
3) For each pixel Z with value q in Q, denote the corresponding pixel in the recovered image R as X and the value of the corresponding pixel Y in L as l, and conduct the following steps.

a) Obtain the same value a as that derived in step 3a of algorithm 1 by applying the same estimation technique used there.

b) Set b to be the value l.

c) Restore p from q by setting

$p= F_a^{-1}(F_b(q))$.

d) Set the value of X to be p.

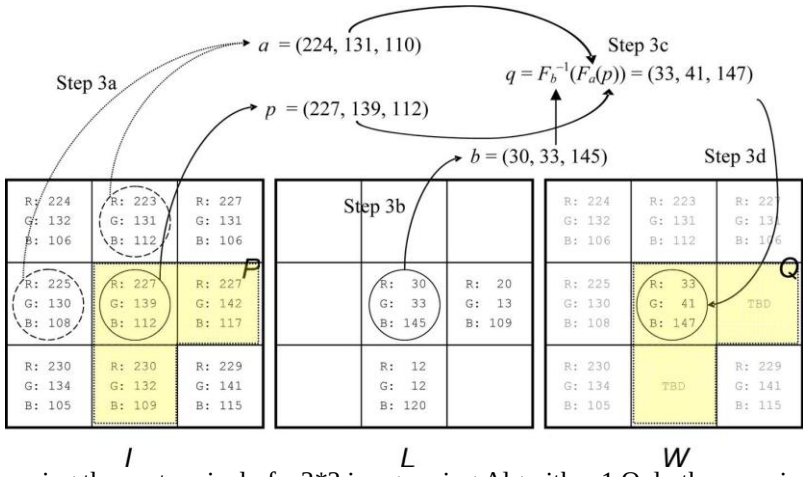

Fig 1.Illustration of mapping the center pixel of a 3*3 image using Algorithm 1.Only the mapping of the center pixel is shown for clarity; the east and south pixels are depicted as TBD (to be determined) in W [9].

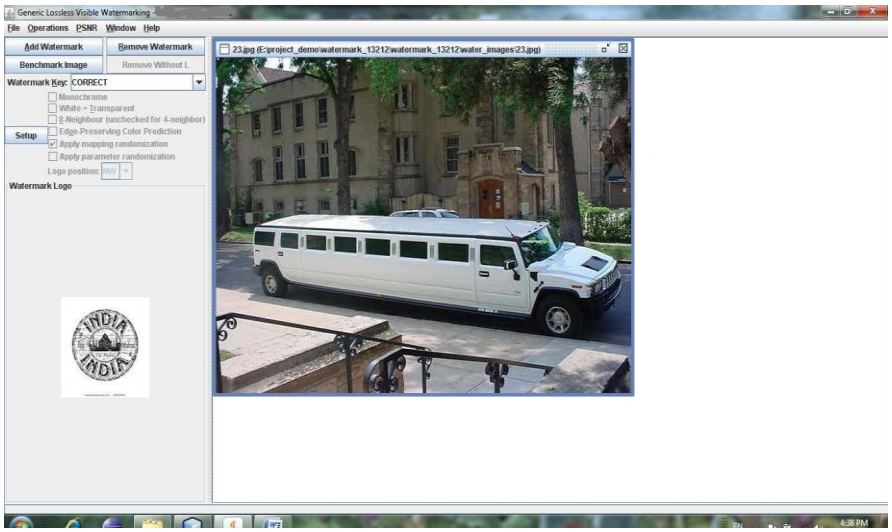

Fig.2.Watermark logo and original Image

Fig. 3. Watermark embedding

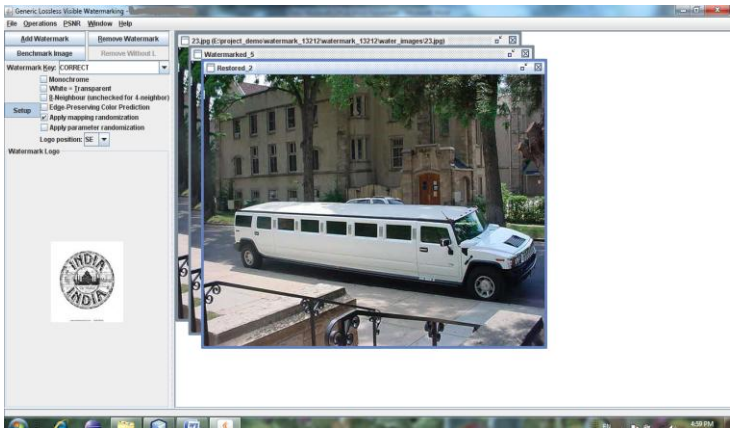

Fig. 4. Watermark removal

4. DATA HIDING USING AES ALGORITHM

The proposed system also includes implementation of tool related to the image processing & where security also applies. Data in the form of text is given as input to our tool, and then it encrypts that data & will be hidden in that image. The image quality remains same, but user will not be able to see that data without decryption. For this, encryption and decryption key will be generated using advanced encryption standard algorithm (AES) [11], [12].Performing data hiding includes two important operations. One is the encode operation, whereby the data in the form of text is inserted into the source image file, and the output is saved in the target image file. The source image file must be of a valid JPEG file type. Other operation is decode operation, whereby data encoded in the given encoded JPEG image is extracted and saved to the output directory, using the original name of the data file stored in the encoded image

4.1 High-level description of the AES algorithm:

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128bit round key block for each round plus one more.
2. Initial Round

1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. SubBytes—a nonlinear substitution step where each byte is replaced with another according to a lookup table**.**
2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes
2. ShiftRows
3. AddRoundKey

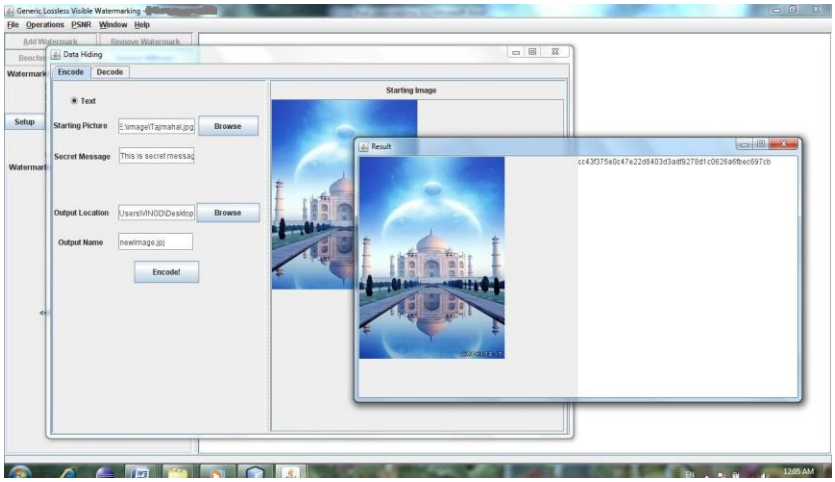

Fig. 5 .Encode operation generating encryption key

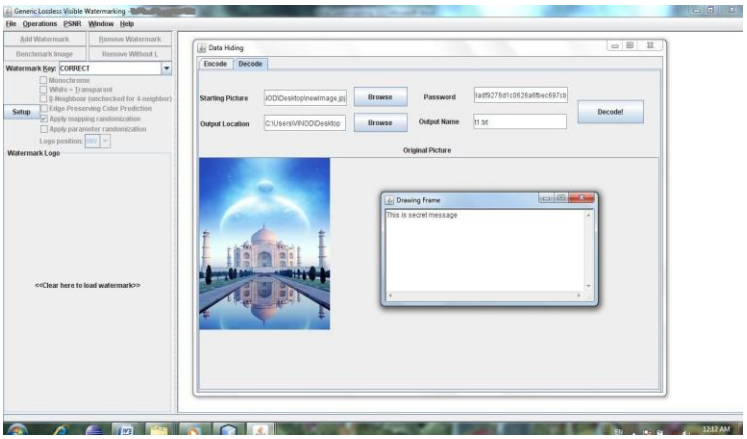

Fig. 6 Decode operation separating original image and text message.

5. CONCLUSION

This paper presents lossless image recovery capability using reversible visible watermarking. This technique uses one-to-one compound mappings that can map pixel values of the image to those of the desired visible watermarks. Hence digital watermarking shows our ownership about that image. After watermark removal, it is possible to obtain lossless image means, original image without loss of pixel. Using AES algorithm, proposed system, hides data to keep the data or image confidential for security purpose.

6. REFERENCES

[1] Y. Hu and S.Kwong,"Wavelet domain adaptive visible watermarking," Electron.Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.

[2] M. Awrangjeb and M. S. Kankanhalli, "Reversible watermarking using a perceptual model," J. Electron. Imag., vol. 14, no. 013014, Mar. 2005

[3] C. de Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Trans. Multimedia, vol. 5, no. 1, pp. 97–105, Mar. 2003.

[4] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

[6] P. M. Huang and W. H. Tsai, "Copyright protection and authentication of grayscale images by removable visible watermarking and invisible signal embedding techniques: A new approach," presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan,R.O.C., Aug. 2003.

[7] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, "Lossless visible watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2006, pp. 853–856.

[8] Raji Pandurangan, E.Logashanmugam, 3T.V.U.Kiran Kumar, "Hardware implementation of visible watermarking," in Proc. IEEE Int. Conf. Computation of power, energy, information and communlcation,2015.

[9] Tsung-Yuan-Liu,Student Member, IEEE, and Wen-Hsiang Tsai, Senior member,"Generic Lossless Visible Watermarking—A New Approach" IEEE Transactions on IMAGE PROCESSING, National Chiao Tung University, Hsinchu 300,Taiwan,R.O.C,VOL.19,NO.5,MAY 2010

[10] P. Kadam, M. Nawale, A. Kandhare, M.Patil, "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique," in Proc. IEEE Int. Conf. Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 2013.

[11] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[12] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#High-level_description_of_the_algorithm.