Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol 2, No 3

Secured Overlapping Technique for Digital Watermarking

Muhammad Sharif (Corresponding author)
Department of Computer Science, COMSATS Institute of Information Technology
PO box 47040, Wah Cantt, Pakistan
Tel: +92303-5188998 E-mail: muhammadsharifmalik@yahoo.com

Aisha Azeem, Waqas Haider, Mudassar Raza
Department of Computer Science, COMSATS Institute of Information Technology
PO box 47040, Wah Cantt, Pakistan
E-mail: aishaazeem19@gmail.com,waqasbtn@gmail.com, mudassarkazmi@yahoo.com

Abstract

Information security is a mandatory issue in current information technology world. A secure overlapping method is proposed in this paper whose key functionality is to distribute the key words at different places inside an image. It requires the extraction of overlapping blocks of image of the size of 4x4 matrixes and taking its transpose. Afterwards arranging the block to linear form row-by-row and applying watermark on it, and finally converting the block back to its original form just like the first step. This technique results in the distribution of hidden data within the block. This scattering of data is beneficial because attacker is unable to find the precise localization of hidden data within the overlapped blocks.

Keywords: Watermarking, Copyrights, Information security.

1. Introduction

Copyright deals with an objects ownership. If the original work is not protected by copyright, then placing digital contents like images or videos on Internet can put them at risk of theft or alterations. Digital watermarking provides a way to handle such issues. The need to protect the work can be depicted from following scenario: Suppose a designer has created an artwork possibly an image of some sort. He than wants that image to displayed on website. But when that image appears somewhere else on the Internet the designer needs to prove his ownership by demonstrating a difference between the copied and the original image. This could be verified easily, if transparent signatures i.e. digital watermarks are embedded within the digital files. These transparent signatures can be noise some random information or possibly sequence of data, so that removal is not possible or is difficult (Vovatzis etc 1999, Chang etc 1999 and Chun 2011).

In this paper different watermarking techniques are reviewed and later a new technique is proposed, in which after the extraction of blocks and applying transpose on it; it is watermarked. The process of taking transpose is key reason of distributing the hidden data in the image. This results in confusing the attacker about the sequence of data and size of block. The rest of the paper is organized as in Section 2 existing techniques in the domain of water marking and features of water marking are reviewed. Section 3 expresses the proposed method for water marking.

2. Classification and Existing techniques of water marking

There are two domains of digital watermarking spatial domain and frequency domain watermarking. The frequency domain also called transform domain water marking. In spatial domain the watermark is directly applied to the pixel values. This approach is simple to employ because the watermarking process is simple.

To embed watermark in pixel values makes the changes minute (Liu etc 2011). On the other hand in frequency or transform domain the watermark is applied to the transform domain components of an image. It is more secure and provides shield against signal attacks. Some common transforms for watermarking are Fourier transforms, discrete cosine transform and wavelet transforms (Xiaoli etc 2010, Chih etc 2010 , Xinge 2010 and Guerrini 2011). Now coming towards the main theme of the paper in which different watermarking techniques are referred e.g. many digital watermarking techniques depend upon different sequences which are embedded into the images spectral representation. The Correlation techniques are used to recognize the watermarks (R.G Van 1994 and 1995). There are some watermarks, which improve the image spatial domain directly using DCT coefficients in which only the user is aware of the sequence (J.F Delaigle 1996). Another approach in which before marking, image is passed through a sub-band filter this is done by spectrum based technique presented in (F.M Boland 1995). While there are other watermarking techniques which rely on images content and hence increase the watermark leveling image . While, still others make use of Human Visual System (Mitchell etc 1996). Another technique is Addition of M-sequences which is presented in (Ray etc 1996) which makes use of linear feedback register to generate binary sequences that has autocorrelation properties. The watermark generated by the linear feedback register is arranged in suitable block, which is then, embedded in the image pixel values. The drawback listed in this technique is that if consecutively bits are known then obviously an attacker can compute the embedded watermark . Based on this, and studying other techniques in next section a new interleaving technique for water marking is proposed.

3. Proposed Technique

The proposed technique tries to overcome an important problem mentioned earlier that arises because of the consecutive placement of digital signature. So In order to avoid this trouble, an interleaving technique is suggested, in which watermark in not kept in consecutive bits, rather it is distributed in different overlapped blocks of image. Whole process of extraction and marking are shown in the flowchart (see figure 1).

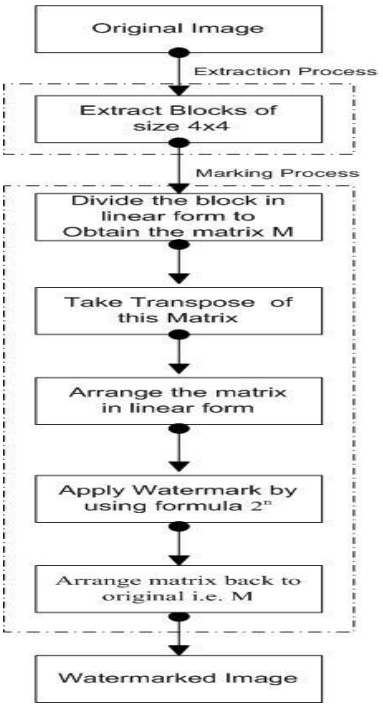

Figure 1. Flowchart of the process

Extraction of the block is the initial step of the proposed technique in which to mark an image, a block X of size 4x4 matrix is extracted from original image as shown in Figure 2. Equation 1 is used to determine the total number of blocks that will be formed in any particular image.

$$B_T = \sum_{T=1}^{N} (r * c)_T / (r + c)_T \text{.....(1)}$$

Where B is the total number of blocks, T is the total number of blocks as 1…N, ***r*** and *c* are the rows and columns respectively.

S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}
S_{25}	S_{26}	S_{27}	S_{28}	S_{29}	S_{30}	S_{31}	S_{32}
S_{33}	S_{34}	S_{35}	S_{36}	S_{37}	S_{38}	S_{39}	S_{40}
S_{41}	S_{42}	S_{43}	S_{44}	S_{46}	S_{46}	S_{47}	S_{48}
S_{49}	S_{50}	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}
S_{57}	S_{58}	S_{59}	S_{60}	S_{61}	S_{62}	S_{63}	S_{64}

Figure 2: Extraction of block 0 from image

After extracting the block X it will undergo following operations.

The block is divided into row-by-row manner as shown below:

$$\mathbf{M} = \begin{pmatrix} S_1 & S_2 & S_3 & S_4 & \text{:L1} \\ S_9 & S_{10} & S_{11} & S_{12} & \text{:L2} \\ S_{17} & S_{18} & S_{19} & S_{20} & \text{:L3} \\ S_{25} & S_{26} & S_{27} & S_{28} & \text{:L4} \end{pmatrix}$$

Where M is the matrix, L1, L2, L3 and L4 are corresponding rows that are divided, and the elements of the matrix are the pixel values of the block. Above-mentioned matrix can also be represented as:

$$M = [A_{i.j}] \text{.....(2)}$$

Where i=1, 2, 3, 4 and j=1, 2, 3, 4 to address rows and columns. Second step of the marking phase is to take the transpose of the matrix M as shown in figure 3 i.e.

$$M^T = [A_{i.j}] \text{.....(3)}$$

S_1	S_9	S_{17}	S_{25}
S_2	S_{10}	S_{18}	S_{26}
S_3	S_{11}	S_{19}	S_{27}
S_4	S_{12}	S_{20}	S_{28}

Figure 3: Transpose of matrix M

After taking the transpose, arrange the image in linear form (i.e. 1-D) and apply watermark W in four consecutive bits obtained from the marking according to equation 4 and figure 4 shows this step.

$$WM = \sum_{b=0}^{n} \left[\sum_{c=0}^{3} X_{bc} + W \right] \text{.....(4)}$$

Where WM is the water marking function, X is the original block and W is the watermark, *b* is the number of block and *c* is the number of bits in a particular block which are extracted and first four bits will be marked and so on the process will be continued up to nth block.

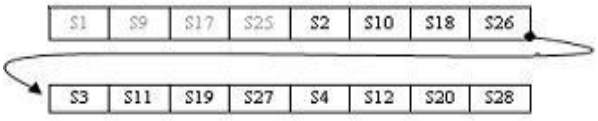

Figure 4: Marking of first four bits

After taking the transpose and applying the watermark arrange the matrix back to its original form i.e. form the matrix M again but this time it is watermarked as shown in figure 5.

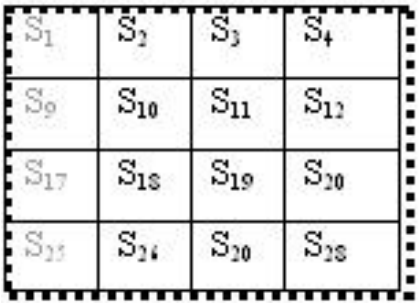

Figure 5: Block 0 watermarked

These operations do not place the watermark bits consecutively; rather it's distributed in different rows of the block. Next time an overlapped block is obtained i.e. it overlaps on the last column (or row) of previous block as shown in figure 6 and hence the process continues i.e. extracting blocks and applying above-mentioned operations until whole image is covered.

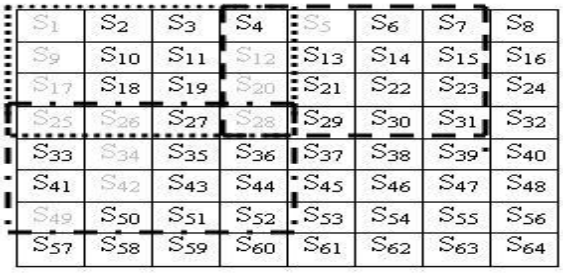

Figure 6: Image after watermarked

3.1 Example

Suppose "WATERMARKING" is the signature to be embedded in the image, for this apply the above-mentioned operations. The step wise process is applied as shown in the following figures (7-10).

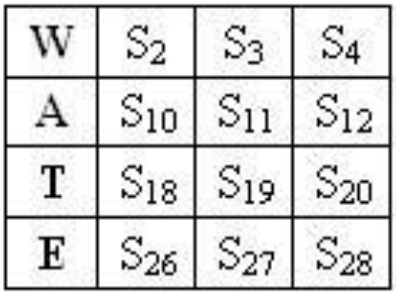

Figure 7: Watermark on block 0

S_4	R	S_6	S_7
R	S_{13}	S_{14}	S_{15}
M	S_{21}	S_{22}	S_{23}
A	S_{29}	S_{30}	S_{31}

Figure 8: Watermark on block 1

S_{25}	I	S_{27}	S_{28}
S_{33}	N	S_{35}	S_{36}
S_{41}	G	S_{43}	S_{44}
K	S_{50}	S_{51}	S_{52}

Figure 9: Watermark on block 2

After embedding the watermarked blocks in the image it will look like this (see figure 10):

W	S_2	S_3	S_4	R	S_6	S_7	S_8
A	S_{10}	S_{11}	R	S_{13}	S_{14}	S_{15}	S_{16}
T	S_{18}	S_{19}	M	S_{21}	S_{22}	S_{23}	S_{24}
E	I	S_{27}	A	S_{29}	S_{30}	S_{31}	S_{32}
S_{33}	N	S_{35}	S_{36}	S_{37}	S_{38}	S_{39}	S_{40}
S_{41}	G	S_{43}	S_{44}	S_{46}	S_{46}	S_{47}	S_{48}
K	S_{50}	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}
S_{57}	S_{58}	S_{59}	S_{60}	S_{61}	S_{62}	S_{63}	S_{64}

Figure 10: Showing distribution of marked signatures
within overlapped blocks

This procedure shows that for an attacker the view will be completely different as compared to the designer because he is unaware of the marking process. In case of attacker if he were to extract the first block he would take the sequence row by row and extract the watermark, in doing so he would also extract the overlapped mark, which is not the proper way. This overlapping is done to make the attacker confuse about the block size and order of sequence. His view about the mark will look something like this: “WARTMEIA ”. This is not the case. Hence, attacker cannot extract the actual order of the embedded signature.

3.2 Verification process

In order to verify that the sequence, which was incorporated in the image for marking, would remain same after extraction, same process is applied as shown earlier in block diagram (see figure 1). Since the designer is to show his claim, obviously he is aware of the whole marking process he would simply extract the first block, take the transpose of it and then arrange it in linear form. This linear arrangement would give the bits that have been marked, he would note it down and same process would continue until all the blocks are verified, and sequence had been found. If exactly the same sequence is obtained then image is original, but if for some block difference has occurred then one can clearly check that somebody other than the designer has tried to change one's image. Graphically the idea is depicted below; first block 0 is extracted from marked image figure 10. Take transpose of it and arrange it in linear form, this linear arrangement will give the bits that have been marked as shown below (see figures 11-15). The same process is applied to all the blocks.

W	S_2	S_3	S_4
A	S_{10}	S_{11}	S_{12}
T	S_{18}	S_{19}	S_{20}
E	S_{26}	S_{27}	S_{28}

Figure 11: Watermarked block 0

W	A	T	E
S_2	S_{10}	S_{18}	S_{26}
S_3	S_{11}	S_{19}	S_{27}
S_4	S_{12}	S_{20}	S_{28}

Figure 12: Transpose of watermarked block 0

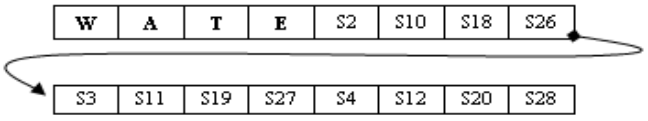

Figure 13: Linear arrangement of block 0 after taking transpose

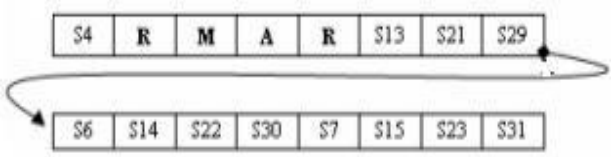

Figure 14: Linear arrangement of block 1 after taking transpose

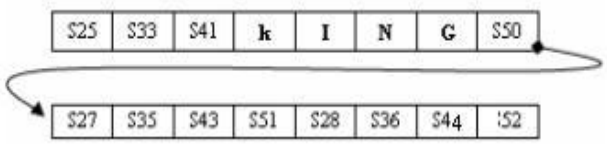

Figure 15: Linear arrangement of block 2 after taking transpose

All the operations were performed to randomly distribute the watermark within different blocks of the original image. If it were not done then the attacker would have been able to obtain the signature embedded. Since overlapping is applied; its basic idea was to confuse the attacker about the size of the block and also the signature which is incorporated into the block. This overlapping results in embedding of signatures from different blocks within each block. As a result attacker would take these as one whole sequence which is distributed in the block, which is not the case.

4. Conclusion

Watermarked signatures are embedded in the overlapping blocks, in which the placement of these signatures is interleaved. By interleaved it means that the embedded mark is not placed consecutively rather it is distributed. Another important point is that the use of overlapped blocks plays a major role in the scattering of signature. As far as the adversaries are concerned, it is not easy for them to find out about the actual order of the embedded mark. The reason being is that, the overlapping blocks confuse the attacker about the block size and secondly the distribution of the embedded signature. Hence, making the proposed scheme secure which scatters the marked sequences in overlapping blocks to confuse the attacker about the block size and the sequences which are incorporated within the blocks. It also provides precise localization for image alterations. The idea's required goal is to protecting images from forgery.

References

Voyatzis, G.; Pitas, I, 1999." Protecting digital image copyrights: a framework". IEEE Journals Computer Graphics and Applications, pp 18 – 24.

Chang-Hsing Lee; Yeuan-Kuen Lee, 1999." An adaptive digital image watermarking technique for copyright protection". IEEE Journals Consumer Electronics. pp 1005 – 1015.

Ming Chen; Zhenyong Chen; Xiao Zeng; Zhang Xiong, 2010."Model Order Selection in Reversible Image Watermarking". IEEE Journal of Selected Topics in Signal Processing. Page(s): 592 – 604

Chun-Hsien Chou; Kuo-Cheng Liu, 2010 ." A Perceptually Tuned Watermarking Scheme for Color Images". IEEE Transactions on Image Processing, pp 2966 – 2982

Liu, F.; Wu, C.-K, 2011. "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners". IET Journals, pp 121 – 128

Xiaoli Li; Krishnan, S.; Ngok-Wah Ma, 2010." A Wavelet-PCA-Based Fingerprinting Scheme for Peer-to-Peer Video File Sharing". IEEE Transactions on Information Forensics and Security, pp 365 – 373

Chih-Chin Lai; Cheng-Chih Tsai, 2010." Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition". IEEE Transactions on. Instrumentation and Measurement. Page(s): 3060 – 3063.

Xinge You; Liang Du; Yiu-ming Cheung; Qiuhui Chen, 2010." A Blind Watermarking Scheme Using New

Nontensor Product Wavelet Filter Banks". IEEE Transactions on Image Processing, pp 3271 – 3284.

Guerrini, F.; Okuda, M.; Adami, N.; Leonardi, R, 2011. "High Dynamic Range Image Watermarking Robust Against Tone-Mapping Operators". IEEE Transactions on Information Forensics and Security, pp 283 – 295

R. G. van Schyndel, A.Z.Tirkel, N.R.A Mee, C.F. Osborne, 1994 . "A digital watermark," Proceedings of the IEEE International Conference on Image Processing, Austin Texas, USA ,vol. 2, pp. 86-90

R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne, 1995. "Towards a robust digital watermark," Proceedings of the ACCV Conference University, Singapore.

J.-F. Delaigle, C. De Vleeschouwer, B. Macq, 1996. "Digital watermarking" Proceedings of the IS&T/SPIE Conference on Optical Security and Counterfeit Deterrence Techniques, San Jose, CA, USA .

F. M. Boland, J. J. K. Ó Ruanaidh and C. Dautzenberg, 1995,. "Watermarking digital images for copyright protection," Proceedings of the International Conference on Image Processing and its Applications ,Edinburgh, Scotland, pp. 321-326.

Mitchell D. Swanson, Bin Zhu and Ahmed H. Tewfik, *1996* ."Transparent robust image watermarking," *Proceedings of the Processing*, Lausanne, Switzerland.

Ray Wolfgang and E. J. Delp, 1996."A Watermark for Digital Images," Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland.