Copyright Protection Service for Mobile Images

Dr. Israa Abdul- Ameer Abdul-Jabbar
Computer Science Department, University of technology/Baghdad
Email:ch_israa81@yahoo.com
Dr. Suhad Malallah Kadhim
Computer Science Department, University of technology/Baghdad

Received on: 31/5/2015 & Accepted on: 17/12/2015

ABSTRACT

This paper presents a watermarking protocol that is used for protecting any digital image and working as a copyright registration for any important image to any user who feels his/her image is important. The registration by this server is applied only once for any input image by keeping the date and the time of the registration with secure authentication process. The authentication process combines both the encryption and the digital signature to generate the invisible watermark that will be added to the image and only the visible watermark will be shown on the lower/right corner of the client image.

The proposed protocol has three stages represented by watermark generation, watermark embedding and verification. For the first stage, three steps should be followed to generate a watermark. In the first step, the phone number with international code is encrypted using SHA-1, in the second step, the result of the first step and a watermark text are encrypted using SHA-1 hash function again and the third step encrypts the result of the second step using RSA algorithm. For the second stage of the protocol discrete wavelet transform algorithm is used for watermark embedding. And for the third stage a matching is done between the retrieval watermarks with the decrypted one.

As a result both concepts of integrity and authenticity can be obtained from the proposed protocol, because hash function using SHA-1 is still secure just time so the system is guaranteed to the two parties: the cover originality, safe transmission with full integrity, and full authenticity.

Keywords: watermarking protocol, SHA-1 hash function, RSA and DWT

INTRODUCTION

Watermarking is needed in mobile devices such as mobile phones and digital cameras, since the security services on these devices are very important [1].

Many watermarking methods and approaches have been proposed in the past few decades [2][3][4]; however, digital watermarking methods for mobile devices are terrible. Some researchers produced watermarking schemes that can be applied to mobile phones [3][5][6]. The

https://doi.org/10.30684/etj.34.4B.1
2412-0758/University of Technology-Iraq, Baghdad, Iraq

watermarking information can be text, signatures or random sequences. For images captured by a mobile phone camera the best watermark information is the digital phone number including the international code. This is because there is a unique phone number for each person all over the world [7].

An optimal digital watermark should be invisible to the viewer, robust to pass through signal transformations, and harsh to remove without reducing the fidelity of the image. Digital watermarks should be established to survive image transformation and compression [8][9][10].

A desirable and a secure watermarking protocol is one which uses the digital watermarking technique and a public key cryptosystem to protect the multimedia when transmitted through digital transaction. current researches denotes that a well secured watermarking protocol should be able to solve at least the following problems:(1)The piracy tracing,(2) The customer right,(3) The binding,(4) The anonymity,(5) The conspiracy,(6) The dispute[11].

This paper produces a watermarking protocol that presents a visible watermark on the lower/right corner of the image, in addition to embed the invisible watermark inside the image. The invisible watermark is generated from encrypted a secret key, digital signature with plain text (watermark text). The benefit of the invisible watermark is to protect the image from attacker [14][15], since if the visible watermark is attacked and disturbed by the attacker The invisible watermark is used as digital signature which is unique to any client that registered his/her image because it is containing the user phone number.

Existing protocols encrypt the watermark and the content with public key cipher and perform embedding under encryption. These protocols create a large computation and bandwidth overhead when used for protecting multimedia data [8][12][13].

The aim of this paper to secure the image of mobile device by a robust watermarking protocol and this can be done by:

- Overcome the limitation of mobile device by using a high level of computations (A time/memory tradeoff)
- The proposed system suggests a watermarking protocol that consists of a combination of watermarking and fingerprinting to provide copyright protection to mobile image when transmitted in wireless environment.

The proposed Watermarking Protocol

The proposed work protects a mobile image by embedding a digital visible watermark. The server provide a remote protection service to any client that contact the server using his/her own mobile device, and the server adding the watermark to the image from its place on client web site when the client request this service from the server. The server achieves the registration process and asks the user to fulfill its unique phone number, the secret key and the information (watermark) to be added in the image.

The service system has three tiers: the first one is the client tier represented by client mobile device, the second one is server tier that consist of Active Server Pages (ASP), and the third tier is oracle database tier to register all client information on the server.

The proposed protocol merges web technologies represented by ASP.net with the concept of invisible watermark to design and implement web watermarking system. This work focuses on the development of watermarking protocol that uses the visible watermark as a tool to protect the copyright of the image and uses digital signature [16] with the exponential cipher encryption [17] method as invisible watermark which is embedded using Discrete Wavelet Transform (DWT) method.

The robustness of this protocol is represented by secure server database with the inability of the intrusion to access the server and tamper the information (client account) stored on server database. The proposed protocol has three stages: watermark generation, watermarking embedding and verification.

Watermark Generation Stage

Three steps should be followed to generate a watermarking:

In the first step, the phone number with international code is encrypted with SHA-1. The proposing of this step is to generate a key that used as digest.

For example suppose the phone no. is +964-07703998110 then

The hash value using SHA-1 will be:

60bf4ab9c7b606c43b799c36ef10babe3ccb3b37.

In the second step, the result of the first step and a watermark text are encrypted using SHA-1 hash function.

For example suppose a text is: CS-UOT then the hash value will be:

b21ed607e7224092e34cde6adcb6d8ae24d23c6c.

Finally, the third step encrypts the result of the second step using RSA algorithm.

Watermark Embedding Stage

This is the second stage in the protocol and it's consisting of embedding the watermark that was generated. Discrete Wavelet transform watermarking technique will be used to add this watermark to image [18] [19]. Algorithm 1 summarizes the steps to embed a watermarking

Algorithm (1): Watermarking Embedding.

Input: cover image and the cipher text.

Output: Watermarked image.

Process:

1. Read and display the cover image and determine its size.
2. Read the text message, determine its size and reshape to vector.
3. Decomposed the Cover image into one level of decomposition using Haar Discrete Wavelet Transform.
4. Embed the cipher text to Horizontal (H2), vertical (V2) & (D2) sub bands when message is 0 & 1.
5. Apply IDWT to the embedded image.
6. Show the Watermarked image.

Watermark Extracting and Verification Stage

The aim of this stage is to extract the embedding watermarking from the image. The following reverse stages are done to extract the watermark.

In this stage we will reverse the previous steps as in algorithm (4):

Algorithm (2): Watermark Extracting

Input: watermarked image, secret key and user phone number.

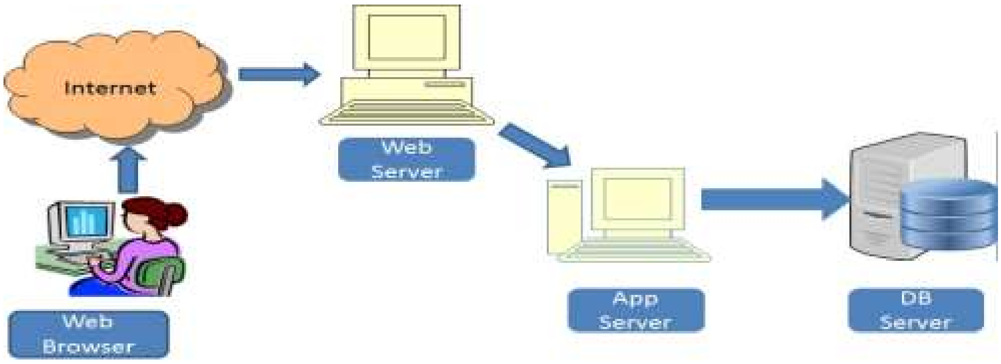
Output: the invisible watermark

Process:

```
1.    Read the encrypted text.
2.    Retrieve the watermarking text and decrypt it.
3.    Compute the hash value for phone no. and watermarking text.
4.    Compare the result of step 3 with step 2
If it is not equal then
  There is a tamper
Else
  Extract watermarking
```

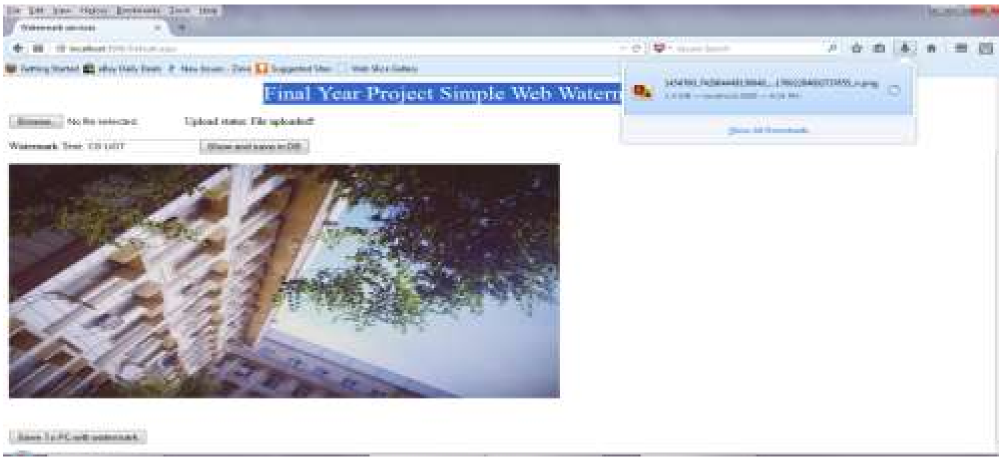
Experiments and Results

The connection between the client and the server is established, as depicted in figure (1).



Figure(1) Client\ Server established connection

The client uploads the image that he/she wants to add watermark to it by entering to embedding web page and follow the instruction in this page. For example to show the embedding process for the image of computer science department/University of Technology are uploaded with the visible watermark CS-UOT as indicated in figure (2):


Final Year Project Simple Web Watern

No file selected. Upload status: File uploaded!

Watermark Text: CS UOT

Figure (2) Downloading the image to server

Set of processing are applied invisibly to the client. After the server completes the encryption, the generating of the signature, and saving all the information in the database, the watermarked image is shown on the client side. Figure (3) shows the watermarking image.

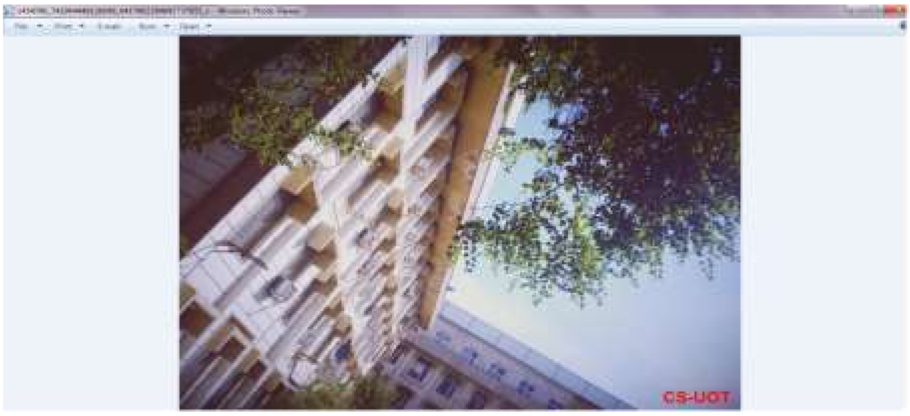


Figure (3) the watermarked image

Discussion

The work proposed watermarking protocol that uses the concepts of digital signature, encrypting and watermarking to produce copyright protection protocol.

The digital signature is used to verify the original owner information, and in this step only the 11 integer value (07703998110) represented by the user phone number with the two symbols (+,-) and 3 integer values of the International code (for example the international code of Iraq is +964-) is used, the whole 16 values will be used as a hash value.

The encryption is used to encrypt this digital signature (MAC) with the watermark to be added in the image (any text selected by the user) are encrypted using RSA cipher. Then the cipher text will be embedded inside image.

The implementation process of the SHA-1 is implemented twice but there is no wasted time because only a little code are entered to this function, then the result of SHA-1 is enciphered very fast. The following table (1) shows the execution time computation:

Table (1): time execution

Processing	Time in seconds
Both SHA-1 & RSA	50.91
Image uploading on server	24.56
Total execution time	75.47

For embedding process oracle database is used to save all the client information that represented by the user phone number, the secret key and the watermark text he/she want to embed in the image. After the client request the service from the server and fulfill all the information, the server starts its process and save the MAC, the Digest2, the encrypted watermark, in addition to connection date and time when the user accessing the server. For extracting and verifying process the server repeats the whole process to extract the embedded-encrypted watermark and reverse its job to get the Digest2 and the MAC to be matched with previously stored information in the database to verify the authenticated user. The information that stored in the server is ready to extract at any time by server and the access is done quickly with no wasted time and the use of separated database will save the memory storage space on server site. In another word we can say, the server processes can overcomes the problem of time and memory tradeoff by producing secure with full authenticity service in just one or two minutes.

The implementation time is reasonable to add enciphering watermark that will be robust enough since if the attacker extracted it from the image, it will be encrypted (not clear) and if tried to disturb the watermarked image by removing the visible mark that shown on the down/right of the original image, the attacker will fail to extract the embedded one and may be deceived by the visible one and cannot imagine there is another invisible watermark embedded in the image.

CONCLUSIONS

1. In the embedding process: we decided to encrypt the watermark (as text) along with SHA-1hash function.

2. In the extracting and verifying process: we will extract the encrypted watermark from the cover (mobile image) using DWT then decrypting the MAC with SHA-1 to verify the mobile phone.

The watermark is robust enough because any attack on the visible watermark will be discovered by generating the digital signature and any mismatch with the encrypted text in this process will show the faking of the attacker. In addition to the robustness of this protocol is represented by secure server database that prevent the intrusion to access the server and tamper with the client account that created and stored on server database.

The authentication process that this server performed is integrated and full secure because the user should fill all the information that the server asked in the verification process as user identification process to check the if the user previously connected to this server and created his own account or not, and if the account is matched then the full process that includes the digital signature generating and the decryption process is repeated at any time the user wanted to verify his/her image originality.

REFERENCES

[1] Ernesto Damiani, "Web Service Security", Encyclopedia of cryptography and security (2nd ED.), Springer, 2011.

[2] Benslimane, D. Dustdar, S. Sheth,A. P. " Services Mashups: The New Generation of Web Applications " , IEEE Computing , Vol.12,No.5,2008, pp. 13-15.

[3] Hugo Haas, Allen Brown,"Web Service Glossary", W3C Working Group, Feb.2004.

[4] Jeedlla,J., and Al-Ahmed,H."An Algorithm for watermarking mobile phone colour image using BCH Code ", IEEE GCC Conference and Exhibition (GCC), Dubai, Feb. 2011, pp.303-306.

[5] Micheal P. Papazoglou, "Web Service Principles and Technology", Web Service Basics ,

online book, 2008.

[6] Charlie Obimbo and Behzad Salami,"Using Digital Watermarking for Copyright Protection" INFORMATICA, Vol.17, No.2, 2006, pp.187-198.

[7] Juergen Seitz, "Digital watermarking for digital Media", university of cooperative education, 2004.

[8] Ingemar J.Cox, Matthew L.Miller, Jeffrey A.bloom, Jessica Fridrich and Ton Kalker "Digital Watermarking and Steganography", second edition, Morgan Kaufmann publisher is an imprint of Elsevier, 2007.

[9] I.Cox, J.Kilian, F. T. Leighton and T. Shamoon, "secure spread spectrum watermarking for multimedia" , IEEE Trans .On Image Processing, Vol.(16), No.(12) 1997, pp.1673-1687.

[10] Yuping Hu."A Watermarking Protocol for Privacy Tracing", International Symposium on Electronic Commerce and Security, Aug. 2008.

[11] Katzenbeisser, Stefan, Aweke Lemma, Mehmet Utku Celik, Michiel Van Der Veen, and Martijn Maas. "A Buyer-Seller Watermarking Protocol Based on Secure Embedding",IEEE Transaction on Information Forensics and Security,Vol.3, No.4, 2008, pp.783-786.

[12] Melinos Averkiou, "Digital watermarking" , Academia.edu, 2010.

[13] I.J.Cox and J.P.Linnartz, "Some general methods for tampering with watermarks" , IEEE Trans. On Selected Area of Communications, Vol.16, No.4, 1998, pp.587-593.

[14] Jyoti Roni, Anupam, "Digital watermarking: comparing two techniques", International Journal of Advanced Research Computer Science and Technology, Vol.2, No.2, 2014, pp. 218-219.

[15] Muna Ghazi, Hanna M. A. Salman, "Secret Sharing Scheme Based Technique for Authentication of Documents Images", Eng. & Tech. Journal, Vol.32, Part (B), No.6, 2014.

[16] V. Rijmen and E. Osward. "Update on SHA-1", RSA Crypto Track, 2005.

[17] "Exponential and RSA Ciphers", Quantitative Reasoning: Computers, Number Theory and Cryptography, V55.0106, pp1-5. Available at http://www.math.nyu.edu/faculty/hausner/rsa.pdf

[18] Ammar Fakhri Mahdi, "Hybrid Algorithm to Improve Robustness of Image Watermarking", Eng. & Tech. Journal, Vol.33, Part (B), No.3, 2015.

[19] Pallavi Patil, D.S. Bormane, " DWT Based Invisible Watermarking Technique for Digital Images" International Journal of Engineering and Advanced Technology (IJEAT), Vol.2, No.4, 2013,pp.603-605.