A SECURE WEB BASED WATERMARKING SCHEME

Nidal F. Shilbayeh*, Sameer A. Nooh
* Department of Computer Science, University of Tabuk, Umluj, Saudi Arabia

DOI: 10.5281/zenodo.3632555

KEYWORDS: Copyright protection; public key infrastructure; watermarking protocol; authentication; web-based security; public key cryptosystem.

ABSTRACT

Applying watermarking protocols can effectively support the copyright protection to identify illegal distributors over the World Wide Web. Several schemes have been developed for copyright protection of the web based digital contents distributed over the internet. However, these protocols are often needs more complex security actions to be performed by the web based content providers for preserving the integrity of their content. In this paper, we propose a new secure web-based watermarking scheme based on the combination of the security of the public key cryptosystem (PKI) and the watermarking based on threshold cryptography. The proposed watermarking protocol solve the collude problem for the trusted certificate authority (CA) and applies the idea of the zero knowledge proof for verification purposes. Implementation and analysis of the proposed scheme has been conducted.

INTRODUCTION

Security, authentication, and copyright protection have become one of the most important problems in research for both web users (U) and content providers (CPs). Consequently, many methods have been developed for copyright protection.

Digital watermarking [1-3] is one of the most appropriate techniques aimed for implementing copyright protection of digital content distributed on the Internet. Most of these watermarking applications focuses on using invisible watermarks that are based on the imperfection of human vision [4]; whereas visible watermarks contains a company sign or logo indicating the rightful ownership of the message or the image [5].

In the literature, most watermarking research techniques concentrate on protecting copyright of legal content providers and tracking improper use of digital content that is owned and then distributed by content providers (CPs) [6-8]. The embedded watermark must be difficult to remove and immune to multimedia data operation Analog to Digital (ATD) [9], Digital to Analog (DTA) [10], dithering [11], and others techniques [12-13] that have been designed to resist tampering and to support the recovery of the rights information originally embedded in the document.

Our contributions can be summarized as follows:

- Developing a secure and authenticated web base watermarking scheme that enables the content providers (CPs) and web user (U) to authenticate each other and make sure all whose claim to be in a secure way.
  - Based on the combination of the security of the public key cryptosystem (PKI) and the watermarking based on threshold cryptography.
  - Assure a non-repudiation service by a CP and a web user.
  - Relying on cryptographic zero knowledge proof for verification purposes.
  - Solving the collude problem for the trusted certificate authority (CA).
- Implementation and evaluation have been conducted.

This paper is organized as follows. Section II presents necessary background information and the related works. The proposed secure watermarking scheme is provided in Section III. In Section IV, we provide the implementation and the analysis results. Finally, we present the conclusion and future work in Section V.

BACKGROUND AND RELATED WORKS

2.1 Entities and Roles

IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.1, January 2019 2
The entities and of the roles of the proposed watermarking scheme includes the following:

1. Web user (U): The people who are using the internet and searching for specific information. the proposed scheme should ensures that the obtained information is correct and provided by an authenticated contents provider (CP) to an authorized party (not a disputer).
2. Content provider (CP): website or organization that handles the distribution of online content. This content is generally made accessible to web users and often in different formats. A content provider responsible for providing a specific services to the interested users and manages access to a central repository of data.
3. Watermark certification authority (WCA): A trusted authority that supplies a trusted watermark certificates and ensures the protection and distribution process of the watermark certificates [1].
4. Watermark service provider (WSP): is a specialized web entity responsible for carrying out the dual watermarking protocol execution, along with the double encryption process, under the PKI [1].
5. Certificate authority (CA): A trusted authority that issues and manages a valid homomorphism public key certificate, which contains public and private keys, and stores the issued certificate in its own database.
6. Registration authority (RA): a specialized web entity that verifies the web user identity, and registers private and public keys for them, and keeps them secure in its own database.
7. Anonymizer (intermediaries): a trusted and secure entity that connects each participant entity guarantees a secure transmission among the involved entities.
8. Judge: an entity responsible for verification purposes to submit evidence of unauthorized copies and to ensure authentication and intellectual properties [1].
9. Local anonymous generator: generating keys based on a specific input, which can be considered as a part of the WSP.
10. Local watermark generator: generating watermarks using a watermark algorithm.

2.2 Related works

In recent years, a number of digital watermarking methods have been proposed. In [14] and [15] proposes a watermarking schemes, which substitute the least significant bits of randomly selected bits of the identification string. Tanaka's scheme [16] proposes quantization noise for protecting the identification code from distortion.

In Craver, Memon, Yeo, and Yeung [17] present solutions to the resolution of the rightful ownership problem and protection of the customer’s rights problem. Jeffrey A. Bloom et al. [18] discuss some proposed solutions and implementation issues for protecting the DVD video.

T. Furon et al. [19] present an alternative asymmetric scheme to classical Direct Sequence Spread Spectrum and Watermarking Costa Schemes. Their method provides a higher security level against malicious attack and can be used for copyright protection.

Nasir Memon et al. [20] propose an interactive buyer-seller protocol for invisible watermarking, in which the seller is not allowed to know the exact watermarked copy that the buyer receives, and their approach prevents the buyer from claiming that an unauthorized copy may have originated from the seller.

Cheung and Chiu [21] presented a distribution protocol to address the management of documents in large enterprises. The protocol uses registration certificates to distribute end user identity information. The intuitive ideas of watermark-based finger printing have been proposed by a number of schemes using cryptographic techniques for the purpose of protecting copyright for the legal content provider.

Dominik et al. [22] presented a framework to monitor media broadcasts utilizing public key infrastructure (PKI) and digital certificates (DC). They proposed an independent monitoring agency to operate the framework and concentrate on IPTV as a new way of delivering audio and video content across IP networks.

Li, Daojing, and Bo Zhang [23] propose a dual watermarking scheme based on threshold cryptography. The proposed algorithm resolves the invisibility and robustness of the embedded watermark. IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.1, January 2019 3

THE WATERMARKING SCHEME

The authors proposed an authentication, non-repudiation, data integrity, robust and security framework. It deploys a public key infrastructure (PKI), digital certificate and dual watermarking based on threshold cryptography along with hash values [24]. The proposed algorithm uses the public key encryption scheme and the RSA because it can be applied with the watermarking schemes for secret watermarking information and authentication purposes.

The public key is for watermark information encryption and the private key is for decryption. By this, the scheme will support the anonymity of the RSA. It is worth mentioning that regarding the RSA public key cryptosystem [25] is a privacy homomorphism with respect to the multiplication operation and another public key cryptosystem that is a privacy homomorphism with respect to the addition operation is presented at [26].

The idea behind the use of the theory of zero knowledge proof at judge and CP side is to identify if the encrypted information is valid by such a party [27].

The algorithm does double encryption using two public keys for the CP and the web user. As a result, no one no one will have the opportunity to know the counterpart watermark information. The CP and the web user will have a public and private key pairs associated with x.509-compliant digital certification issued by a trusted certification authority (CA) [28]. The encryption used the privacy homomorphism property of PKI, with respect to $\oplus$.

Phase 1: Registration Authority (RA) Issued key pairs for the Web User (WU) and the Contents Provider (CP)

The web users (Us) and the contents providers (CPs) should have a pair of keys, (PK_{CP}, SK_{CP}) and (PK_u, SK_u), from the registration authority in order to use them for generating a pair of anonymous keys $(PK^{*}\ , SK^{*}\ )$ and (PK^{*} , SK^{*}). Fig.1 shows how each the web user (U) and the content Provider CP receives their keys from the RA. Fig. 2 shows how the anonymous keys are generated. All messages of transmission are carried over the anonymizer (intermediary) entity to assure secure message transmission.

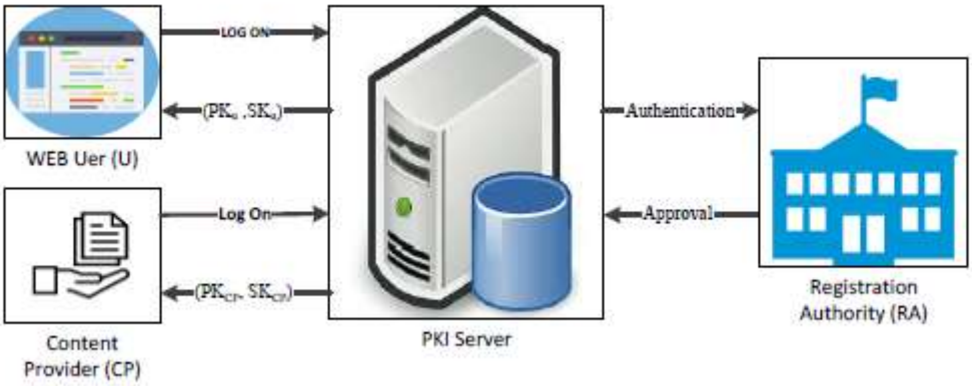


Fig.1 Web user (u) and Content Provider (CP) obtaining their keys

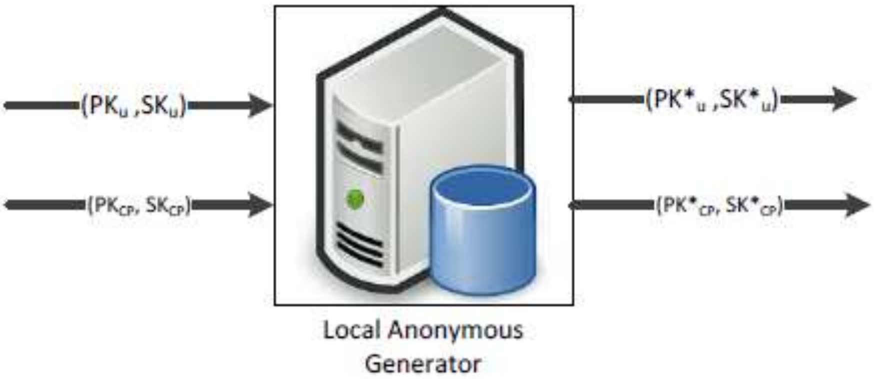


Fig.2 Web user (u) and Content Provider (CP) anonymous keys

Phase 2: Watermark Generation Protocol

- The Web user (U) sends an encrypted request certificate message (EPK*U(WU),PK*U) to the content provider (CP) as shown **process 1** in fig.3 .
- The CP checks its validity using a zero knowledge proof theory.
- The CP sends a watermark certificate request to the WCA as shown in **process 2** in fig.3.
- The CP computes the WCP by hashing the web user request and public key as in eq. 1[38] :
  WCP = H(R) + H(K) (1)
- The CP encrypts the computed WCP using the CP public key to get $EPKCP(WCP)$
- Additionally, a random sequence function, Fq, will be generated
- The CP sends a digital signature request to the CA with the encrypted watermark, $EPKCP(WCP)$, along with CP public key as in **process 3** shown in fig.3.
- The CA hashes the encrypted watermark, $EPKCP(WCP)$, along with CP public key and a timestamp T1 to obtain the tuple TCA as in eq. 2. TCA={ H(E PKCP(WCP), PKCP ,T1), T1} (2)
- A digital signature, DSCA, is obtained by encrypting H(TCA) with the CA private key, (CAPR), and then with the CP public key, as in eq. 3: DSCA(TCA)=E(PKCP(PRCA(H(TCA)) (3)
- The CA then sends the issued certificate CertCP to the CP as in **process 4** shown in fig. 3, using eq. 4: CertCP ={TCA,DSCA(TCA)} (4)
- The CP decrypts the certificate CertCP with the CA public key and with its own private key to obtain H(TCA).
- The CP hashes TCA to get H1(TCA).
- If H(TCA) = H1(TCA) then the issued certificate CertCP has been verified. Otherwise, it's tampered. All issued certificates will be stored in the database for verification.
- The CP sends the certificate CertCP to the Judge (J) for verifying the existence of sensitive information in the watermarking operation as in **process 5** as shown in fig. 3. if verified then do the following:
  - The CP encrypts $EPKU*(Wu)$, WCP and Fq using PKCP, and PK*U.
  - The CP sends the $EPKCP(EPKU*(Wu))$,$EPKCP(EPKU*(WCP))$,$EPKCP(EPKU*(Fq)$ with the issued certificate CertCP to the Watermark Service Provider (WSP) to do double watermarking as in **process 6** shown in fig. 3.
  - WSP do double encryption and do the following:
    $EPKCP(EPKU*(Wcp))\bigoplus EPKCP(EPKU*(WU))$
    $=EPKCP(EPKU*(Wcp\bigoplus WU))$
    $=EPKCP(EPKU*(Wcp\bigoplus WU))$
    $=EPKCP(EPKU*(WCPU))$
    $=EPKCP(EPKU*(WCPU))\bigoplus EPKCP(EPKU*(Fq))$
    $=EPKCP(EPKU*(WCPU\bigoplus Fq))=EPKCP(EPKU*(Fq(WCPU)))$
  - Applying a dual watermarking scheme based on threshold cryptography.

- The WSP sends the $E_{PK_{CP}}(E_{PK_{U^*}}(F_q(W_{CPU})))$ with a dual watermark webpage to the judge for verification as in **process 7** shown n fig. 3.
- If the Judge does the verification using the zero knowledge proof and send it again to the CP as in **process 8** shown in fig.3. In addition to that, the Judge do the following:
- ○ The CP decrypts the $E_{PK_{CP}}(E_{PK_{U^*}}(F_q(W_{CPU})))$ using the SK$_{CP}$ to obtain $E_{PK_{U^*}}(F_q(W_{CPU}))$ and then $E_{PK_{U^*}}(F_q(W_{CPU}))\bigoplus E_{PK_{U^*}}(X)$).
- The CP sends $E_{PK_{U^*}}(F_q(W_{CPU}))\bigoplus E_{PK_{U^*}}(X)$) to the web user as in **process 9** shown in fig.3..
- Finally, the Web user (U) decrypts the $E_{PK_{U^*}}(F_q(W_{CPU}))\bigoplus E_{PK_{U^*}}(X)$) using SK$_{*U}$ to obtain the digital contents $(F_q(W_{CPU}))\bigoplus(X)$).

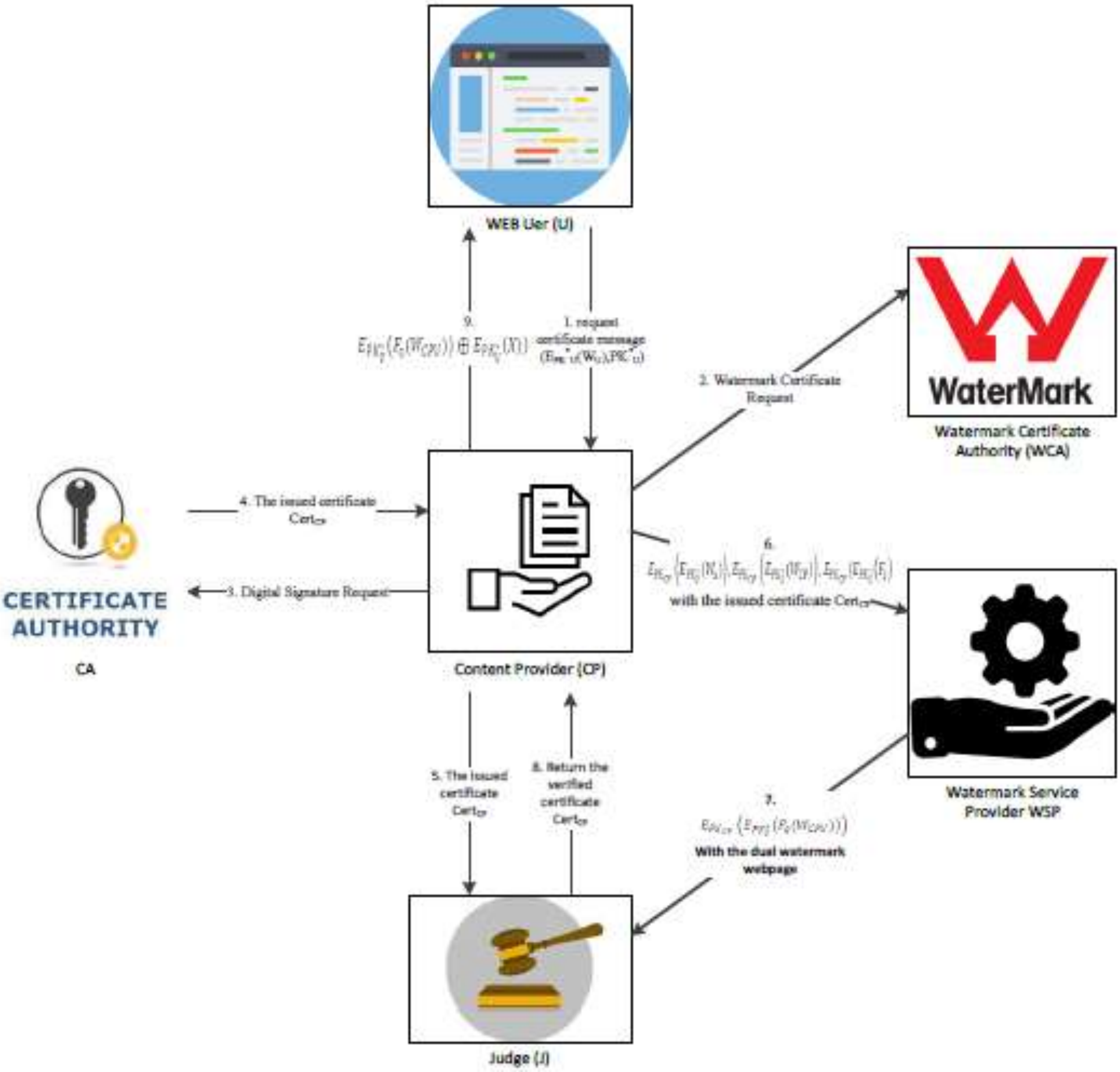

WEB Uer (U)
9.
$E_{PK_U^*}(F_q(W_{CPU}))\oplus E_{PK_U^*}(X))$
1. request certificate message
$(E_{PK^*_U}(W_U),PK^*_U)$
2. Watermark Certificate Request
WaterMark
Watermark Certificate Authority (WCA)
4. The issued certificate
$Cert_{CP}$
3. Digital Signature Request
CERTIFICATE AUTHORITY
CA
Content Provider (CP)
6.
$E_{PK_{CP}}(E_{PK_U^*}(W_U)), E_{PK_{CP}}(E_{PK_U^*}(W_{CP})), E_{PK_{CP}}(E_{PK_U^*}(F_q))$
with the issued certificate $Cert_{CP}$
Watermark Service Provider WSP
5. The issued certificate $Cert_{CP}$
8. Return the verified certificate $Cert_{CP}$
7.
$E_{PK_{CP}}(E_{PK_U^*}(F_q(W_{CPU})))$
With the dual watermark webpage
Judge (J)

Fig.3 Watermark Generation Protocol

IMPLEMENTATIONS

The implementation uses the following simulator ModelSim-Altera 6.0c Software. The encoder has been used for embedding a watermark images associated with the web page as strong evidence for CP authentication. Sensitive information associated with a web page will have higher priority in comparison with the information provided by the CP.

The generated watermark embedded into the tag of the source code of the webpages (HTML). The embedded dual watermarks can be done by moving in both directions horizontally and vertically in the layers.

The scheme depends on the dual watermarking based on threshold cryptography [23]. The following flowchart describes the implementation process.

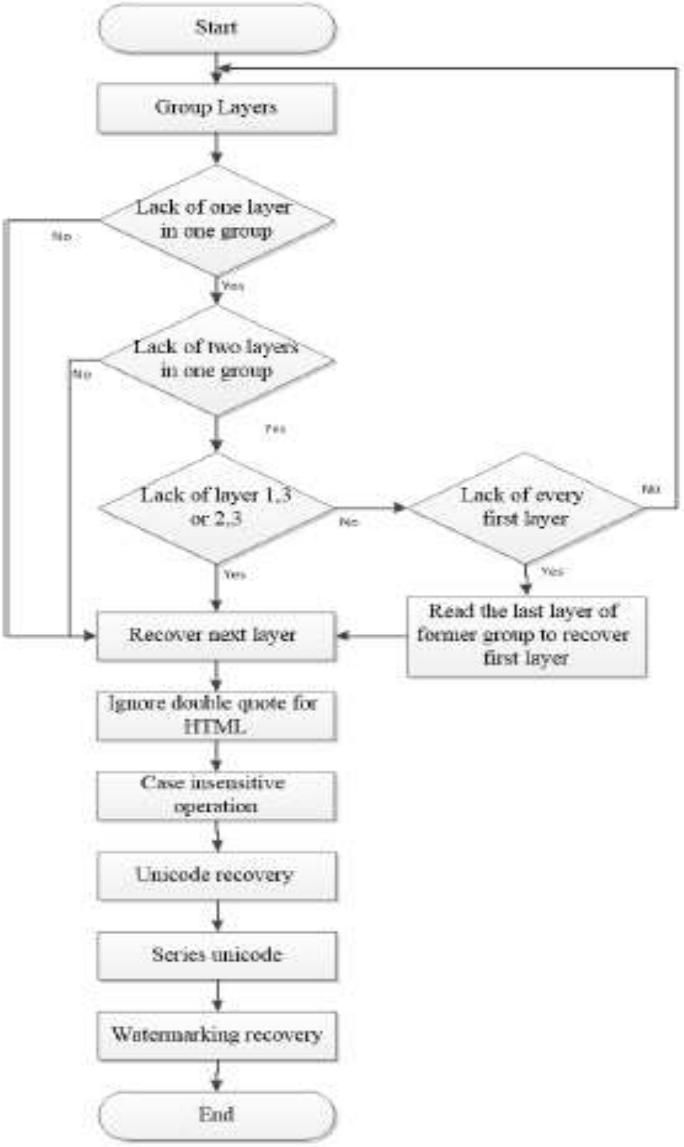

Start
Group Layers
Lack of one layer in one group
No
Yes
Lack of two layers in one group
No
Yes
Lack of layer 1,3 or 2,3
No
Yes
Lack of every first layer
No
Yes
Read the last layer of former group to recover first layer
Recover next layer
Ignore double quote for HTML
Case insensitive operation
Unicode recovery
Series unicode
Watermarking recovery
End

Fig.4 Flowchart for dual watermarking process

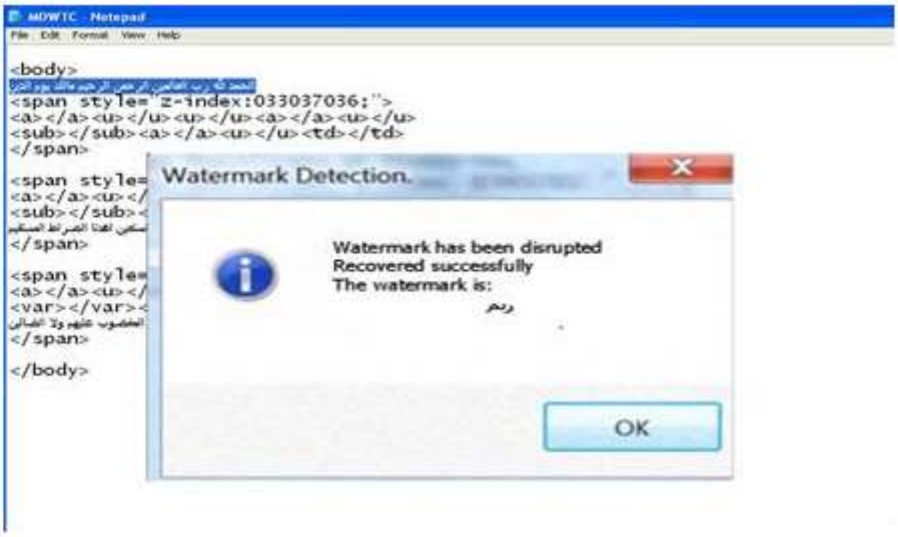
The main distinguishing factor from [23] is that:

- In each layer, combine the first authentication code from the line and the second authentication code from the column of a digital watermark within a layer. Thus the entire watermark could be embedded into the HTML tag.
- Embedding the watermark into the tags of the HTML code using case intensive HTML tags. If any bit in the watermark is 0, then the corresponding character in the tag will be converted into lowercase, otherwise into uppercase, during the recovery process.
- Omit the embedded double quoted parts of the HTML tags to save time for watermark generation process.

In case of some missing layers, the detection process will read the backup watermark stored at the head of the previous layer. For the tampering of webpages, the watermark will be destroyed.

The generated watermark embedded into the tags of the source code of web pages (HTML) by moving along vertically and horizontally in a layer. The proposed scheme has been evaluated in term of:

- Invisibleness: The proposed scheme does not show any visual differences between the original web page and watermarked one.
- Robustness: Specialized software has been used to detect pre and post watermarking in pixel level. The first sentence has been damaged to verify robustness. Fig.5 shows the watermark has been recovered after tampering the web page
- Efficiency: The proposed scheme shows an acceptable watermark embedding time.



```
<body>
الحمد لله رب العالمين الرحمن الرحيم مالك يوم الدين
<span style="z-index:033037036;">
<a></a><u></u><u></u><a></a><u></u>
<sub></sub><a></a><u></u><td></td>
</span>
<span style=
<a></a><u></
<sub></sub><
ستعين اهدنا الصراط المستقيم
</span>
<span style=
<a></a><u></
<var></var><
المغضوب عليهم ولا الضالين
</span>
</body>
```

Watermark has been disrupted
Recovered successfully
The watermark is:
ريم

Fig.5 Watermark detection after tampering the web page

CONCLUSION

The proposed scheme is based on the combination of the security of the public key cryptosystem (PKI) and the watermarking based on threshold cryptography. The algorithm relying on cryptographic zero knowledge proof for verification purposes, Solving the collude problem for the trusted certificate authority (CA), and Assuring a non-repudiation service by the content provider (CP) and a web user (U). The algorithm has been implemented and tested using MODELSIM 6.0a software. The invisibility, robustness and the efficiency has been evaluated and showed tamperproof if the document is damaged.

REFERENCES

1. Shilbayeh, Nidal F., Sameer A. Nooh, and Reem A. Al-Saidi. "An Efficient and Secure Web-Based Dual Watermarking Scheme." IJCSNS 19, no. 6 (2019): 149-158.
2. Shilbayeh, Nidal F., Belal AbuHaija, and Zainab N. Al-Qudsy. "A Robust Hybrid Blind Digital Image Watermarking System Using Discrete Wavelet Transform and Contourlet Transform." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering11.3 (2017): 407–413.
3. Lei, Chin-Laung, Pei-Ling Yu, Pan-Lung Tsai, and Ming-Hwa Chan. "An efficient and anonymous buyer-seller watermarking protocol." IEEE transactions on Image Processing 13, no. 12 (2004): 1618-1626.
4. Holliman, Matthew, and Nasir Memon. "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes." IEEE Transactions on image processing 9.3 (2000): 432–441.
5. Hu, Yongjian, and Sam Kwong. "Wavelet domain adaptive visible watermarking." Electronics Letters 37, no. 20 (2001): 1219-1220.
6. O'Ruanaidh, J. J. K., W. J. Dowling, and F. M. Boland. "Watermarking digital images for copyright protection." IEE Proceedings-Vision, Image and Signal Processing 143, no. 4 (1996): 250-256.
7. Lin, Shinfeng D., and Chin-Feng Chen. "A robust DCT-based watermarking for copyright protection." IEEE Transactions on Consumer Electronics 46, no. 3 (2000): 415-421.
8. Lin, Shinfeng D., and Chin-Feng Chen. "A robust DCT-based watermarking for copyright protection." IEEE Transactions on Consumer Electronics 46, no. 3 (2000): 415-421.
9. Wu, Min, and Bede Liu. Multimedia data hiding. Springer Science & Business Media, 2013.
10. Rhoads, Geoffrey B., J. Scott Carr, and Burt W. Perry. "Digital authentication with digital and analog documents."U.S. Patent 7,770,013, issued August 3, 2010.
11. Tanaka, Kiyoshi, Yasuhiro Nakamura, and Kineo Matsui. "Embedding secret information into a dithered multi- level image." In IEEE Conference on Military Communications, pp. 216-220. IEEE, 1990.
12. Hu, Yongjian, Sam Kwong, and Jiwu Huang. "Using invisible watermarks to protect visibly watermarked images." In 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No. 04CH37512), vol. 5, pp. V-V. IEEE, 2004.
13. Lin, Shinfeng D., Yu-Chan Kuo, and Yu-Hsun Huang. "An image watermarking scheme with tamper detection and recovery." In First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06), vol. 3, pp. 74-77. IEEE, 2006.
14. Klein, Dean A. "Data security for digital data storage." U.S. Patent 6,857,076, issued February 15, 2005.
15. Van Schyndel, Ron G., Andrew Z. Tirkel, and Charles F. Osborne. "A digital watermark." In Proceedings of 1st International Conference on Image Processing, vol. 2, pp. 86-90. IEEE, 1994.
16. Tanaka, Kiyoshi, Yasuhiro Nakamura, and Kineo Matsui. "Embedding secret information into a dithered multi- level image." In IEEE Conference on Military Communications, pp. 216-220. IEEE, 1990.
17. Qiao, Lintian, and Klara Nahrstedt. "Watermarking schemes and protocols for protecting rightful ownership and customer's rights." Journal of Visual Communication and Image Representation 9, no. 3 (1998): 194-210.
18. Bloom, Jeffrey A., Ingemar J. Cox, Ton Kalker, J-PMG Linnartz, Matthew L. Miller, and C. Brendan S. Traw. "Copy protection for DVD video." Proceedings of the IEEE 87, no. 7 (1999): 1267-1276.
19. Furon, Teddy, and Pierre Duhamel. "An asymmetric watermarking method." IEEE Transactions on Signal Processing 51, no. 4 (2003): 981-995.
20. Memon, Nasir, and Ping Wah Wong. "A buyer-seller watermarking protocol." IEEE Transactions on image processing 10, no. 4 (2001): 643-649.
21. Cheung, Shing-Chi, and Dickson KW Chiu. "A watermarking infrastructure for enterprise document management." In 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the, pp. 10-pp. IEEE, 2003.
22. Birk, Dominik, Seán Gaines, and Christoph Wegener. "A framework for digital watermarking next generation media broadcasts." Axmedis 2008 45 (2008): 19.
23. Li, Daojing, and Bo Zhang. "DWTC: A dual watermarking scheme based on threshold cryptography for web document." In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), vol. 8, pp. V8-510. IEEE, 2010.

24. Frattolillo, Franco. "Watermarking protocol for web context." IEEE Transactions on Information Forensics and Security 2, no. 3 (2007): 350-363.
25. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21, no. 2 (1978): 120-126.
26. Cohen, Josh D., and Michael J. Fischer. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, 1985.
27. He, Yong-Zhong, Chuan-Kun Wu, and Deng-Guo Feng. "Publicly verifiable zero-knowledge watermark detection." Ruan Jian Xue Bao(Journal of Software) 16, no. 9 (2005): 1606-1616.
28. Cooper, Dave. "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile." (2008).

Nidal Shilbayeh received the BSc degree in computer science from Yarmouk University, Irbid, Jordan in 1988, the MS degree in computer science from Montclair State University, New Jersey, USA in 1992, and the PhD in computer science from Rajasthan University, Rajasthan, India in 1997. He is a Professor at the University of Tabuk. He was the Vice Dean at university of Tabuk, Saudi Arabia; He was the Vice Dean of Graduate Studies and Scientific Research at Middle East University, Amman, Jordan. He supervised many graduate students for the MS and PhD degrees. His research interests include Security (Biometrics, Identification, Privacy, Authentication, and Cryptography), Information Security (e-payment, e-voting, and e-government), Face Recognition, Digit Recognition, Watermarking, Embedding, Nose System, Neural Network, Image Processing, and Pattern Recognition.

Sameer A. Nooh received the BSc. A degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, and MSc Internet, Computer and System Security from University of Bradford, UK in Information Security in 2007. MSc consultancy from Liverpool John Moores University. Sameer finished his Ph.D. in Computer Science De Montfort University in Leicester, UK 2014. In 2015, Dr.Sameer joined the Computer Science Department, University of Tabuk, as an Assistant Professor in the Computer Science Department, University College, Umluj. His main areas of research interest are Information and System Security, Computer Science, and anything related to the Internet and computer. Since 2014 Dr. Sameer started some administrative assignments includes: Supervisor of Information Technology Unit, Vice-dean of University College, Umluj and now he is Dean of University College, Umluj, University of Tabuk, The northern area, Tabuk, Saudi Arabia.