An Efficient and Secure Web-Based Dual Watermarking Scheme

Nidal F. Shilbayeh[1], Sameer A. Nooh[1], Reem A. Al-Saidi[2]

[1]Department of Computer Science, University of Tabuk, Umluj, Saudi Arabia
[2]King Abdullah Second School for Information Technology University of Jordan, Amman, Jordan

Summary
Advances in multimedia and networking technologies have enabled the infringement of digital content distributed over the internet. Consequently, several methods have been developed for copyright protection to identify illegal distributors through the World Wide Web (WWW). However, no agreed-upon mechanism exists for authenticating content provider websites or for preserving the integrity of their content. In this paper, we propose an effective and secure watermarking protocol that encapsulates a flexible and convenient solution for the content provider (CP) authentication and integrity problem. The security of the proposed protocol is based on the security of (PKI) and dual watermarking based on threshold cryptography. The proposed protocol exploit the existence of the trusted CA to solve collude problem and applying the idea of zero knowledge proof for verification purpose. The analysis results indicate the functional verification for encoder (watermark embedding), decoder (watermark extracting), encryption, decryption and hashing. Additionally, the evaluation results show better results for modified DWTC compared with other schemes (RP, WSC, and SSC) in terms of embedding time for large contents.

Key words:
Copyright protection; public key infrastructure; dual watermarking protocol; authentication; web-based security; public key cryptosystem; Digital to Analog (DTA); Analog to Digital (ATD).

1. Introduction

Thanks to the propagation of the World Wide Web (WWW), a large amount of multimedia content—text, graphics, images, videos, and audio—are available for browsing and downloading by millions of users worldwide over the network. As a result, security, authentication, and copyright issues have become significant problems in research and applications for both web users and website content providers.

Digital watermarking is a promising technology employed for such problems by various digital rights management systems (DRMs) to achieve rights management for digital content distributed over the internet. It supports copyright information (owner identity) for multimedia data to be embedded as unperceivable signals into digital content. The signals can be perceivable or unperceivable to humans. The invisible, unperceivable watermark content appears perceptually identical to the original. A detection algorithm can be used to extract the invisible watermark [1], [2].

Note that most applications focus on invisible digital watermarking techniques for documents that are based on the imperfection of human vision; whereas visible digital watermarks [2] contain an evident visible message or company logo indicating rightful ownership of the image. It should be perceptible enough to discourage theft but not perceptible enough to decrease the utility or appreciation of the document.

On the other hand, digital watermarking techniques can be classified according to the availability of the original object as: blind, semi-blind, or private watermarking [3]. Blind watermarking does not require the original digital object to run the detection and extraction algorithm. In some cases, extra information is required to run this algorithm, which is referred to as semi-blind watermarking. In the private watermarking technique, the original digital object is required, and thus this can only be completed by the legitimate owner.

However, watermarking protocols provide appropriate infrastructure to support the digital rights management process for digital content; to implement effective mechanisms for tracking down improper use of digital content that is owned and then distributed by content providers (CPs) [4],[5]; for media fingerprinting system implementation [6]; for broadcast and advertising monitoring [7]; and for convert channel communication [8].

In the literature, many robust watermarking techniques have been addressed [11], [12], [13]. Most watermarking research techniques [9], [10] concentrate on protecting copyright of legal content providers and tracking guilty users. The watermark must be difficult to remove and immune to multimedia data operation Digital to Analog (DTA), Analog to Digital (ATD), dithering, re-sampling rotation, and others techniques that have been designed in order to resist tampering and to support later extraction and detection of watermark signals that are used to recover the rights information originally embedded in the document. However, nothing protects the authentication, integrity, and non-repudiation services for e-transaction systems.

Our contributions can be summarized as follows:

- Developing a secure and authenticated website framework by enable the CPs and web user to

Manuscript received June 5, 2019
Manuscript revised June 20, 2019

authenticate each other and make sure that both entities whose claim to be in a secure way.

- Assure a non-repudiation service by a CP and a web user, which mean the CP wants to be able to trace unauthorized copies so if an illegal copy is supplied it will be possible to identify such infringement
- Relying on cryptographic zero knowledge proof to make verification of an illegal distributor without watermark information disclosure and validate the encrypted watermark information.
- Developing a dual watermarking scheme under the authenticated framework for the integrity and copyright preservation.
- Make the scheme secure against collusion attack even if third party is not trusted by using a dual watermark technique and double encryption method based on PKI.

This paper is organized as follows. Section II presents necessary background information and related works. The proposed secure and authenticated website framework 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.

2. Related works

In recent years, a number of digital watermarking methods have been proposed. Among the earliest works include L.F Turner's [14] digital audio watermarking methods, which substitute the least significant bits of randomly selected audio samples with bits of identification string. A similar idea has been applied to images [15]. The identification code can easily be destroyed as it depends on the least significant bit, so several other proposals for watermarking, such as Tanaka's scheme [16] that uses the quantization fact, have been proposed.

Brassil's methods [17] adds Caronni's geometric pattern. These schemes are easily defeated using filtering and cropping. Bender, Gruhl, and Morimoto [18] discuss two different approaches to watermarking: (1) patchwork and (2) texture block coding. Patchwork is considered to be statistical, and it is resistant to compression and FIR filters and remarkably resistant to cropping; whereas texture block coding is a visual approach that is limited to images with a lot of texture.

Smith and Comiskey [19] discuss the characteristics of the data hiding scheme, robustness, and amount of data to be hidden, perceptibility, and signal-to-noise ratio. They introduce a new hiding scheme, whose parameters can be adjusted to the capacity, imperceptibility, and robustness.

Koch, Rindfrey, and Zhao [20] present an image watermarking method. The image is grouped into 8 x 8 blocks, and each block is DCT transformed. This method is vulnerable to multiple document attacks.

Cox, Killian, Leighton, and Shamoon [21] argue that a watermark must be placed in perceptually significant components of a signal if it is to be robust enough to handle common signal distortions and attacks. They propose inserting a watermark into spectral components of the data using techniques analogous to spread-spectrum communications, hiding a narrow-band signal in a wide-band.

Hartung and Girod [22] provide a watermarking scheme specifically for the MPEG-encoded video. Their scheme is to apply DCT to each of the 8 x 8 blocks of the watermark and then add Discrete Cosine Transformation (DCT) coefficients of the watermark to the corresponding DCT coefficients of the MPEG stream.

Craver, Memon, Yeo, and Yeung [23], from IBM, address an important issue of rightful ownership. Jeffrey A. Bloom et al. [24] describe the copy protection system currently under consideration for DVD, and they discuss some proposed solutions and implementation issues that are being addressed. Ingemar J. Cox et al. [25] present a secure (tamper-resistant) algorithm for watermarking images and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data.

T. Furon et al. [26] present an asymmetric watermarking method as an alternative to classical direct sequence spread spectrum (DSSS) and watermarking costa scheme techniques, and their method proves that the Kerckhoffs principle can be stated in the copy protection framework.

Joachim J. Eggers et al. [27] have proposed new approaches that are significantly less complex than the public watermark detection principle that works without explicit reference to the embedded signal.

Nasir Memon et al. [28] 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.

R.L. Rivest et al. [29] developed an encryption method with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key.

Neil F. Jhonson et al. [30] propose alternative methods for image recognition based on the concept of identification marks (ID-marks of fingerprints).

Cheung and Chiu [31] 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 [10], [32].

Dominik et al. [32] 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.

I-Shi Lee and Tsai [39] embed special space codes in the HTML text to embed watermarks into the webpage. The codes, replacing the space code ASCII 0x20, appear as white spaces in the HTML text as well, and there are ASCII CODE, such as &#32 and , that are used in this technique. There is no change or impact on display. However, its robustness is low when special space is added, and loss may lead to watermark detection failure. Data hiding using the steganography concept is an efficient means of secret communication. It is convenient to use the webpage as a communication channel by hiding secret messages in the HTML file of a cover webpage due to high accessibility on the internet. The advantage here is that the secret message cannot be destructed illegally unless the HTML file is modified, and the website publishing the webpage is intruded. Regarding hiding data in the HTML, it protects a Java applet in an HTML file from being copied by hiding a special character string with a secret key within the Java applet. Binary data is hidden in the HTML files using various properties of tags, such as attributes for bit encoding.

3. The Proposed Dual Watermarking Scheme

The proposed dual watermarking scheme will be double encrypted using two public keys kept separately by the involved entities. Consequently, no one will have the opportunity to know the counterpart watermark information. The idea behind the RSA public key encryption scheme is that it can be applied to the watermarking scheme for secret watermarking information and also for the characteristic of the Content provider (CP) and web user to prove the authentication property.

Under the PKI, the main involved entities will have a key pair (public and private keys) associated with x.509-compliant digital certification issued by a trusted certification authority (CA) [34]. The encryption function used in the PKI is assumed to be a privacy homomorphism, with respect to the watermark insertion operation $\oplus$ [35]. The privacy homomorphism property of public key encryption, with respect to $\oplus$, means eq. 1 holds for every (a) and (b) in the message space.

$$E_{PKI}(a \oplus b)=E_{PKI}(a) \oplus E_{PKI}(b) \quad (1)$$

It is worth noting that the RSA public key cryptosystem [29] 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, which is presented at [36]. The idea behind the use of the theory of zero knowledge proof on the judge and CP side is to identify whether the encrypted information is valid by such a party [37].

3.1 Entities and Roles

The proposed watermarking scheme is based on the following entities: content provider (CP), web user, server, watermark certification authority (WCA), watermark service provider (WSP), certificate authority (CA), anonymizer (intermediaries), registration authority (RA), judge, local anonymous generator, and local watermark generator.

The description of the roles of the used entities in our proposed dual watermarking scheme includes the following:

1. Content providers (CPs): website(s) spread out through the internet WWW that is responsible for providing a specific service for an interested user. For the designed infrastructure, it may become an Islamic website that provides fatwa or a Quran center provider. Several CPs exit to deliver the content upon request from an interested user.
2. Web user: a person who browses the internet and is interested in specific information. The main goal in the designed infrastructure that ensures that the obtained information is correct and provided by an authenticated CP to an authorized party (not a disputer).
3. Server(s): specialized software that connects CPs with web user(s) to deliver content upon request to different web users.
4. Watermark certification authority (WCA): trusted authority that supplies trusted watermarking certificates to guarantee the entire protection and distribution process for watermark certificates and to ensure correct watermark protocol execution.
5. 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.
6. Certificate authority (CA): an entity that gives a valid homomorphism public key certificate, which contains public and private keys, and maintains the issued certificate in its own database. Each legitimate certificate must be issued by a trusted PKI certification authority.
7. Anonymizer (intermediaries): a trusted secure entity that connects each participant entity to assure secure

data transmission against attacks. It guarantees a secure transmission among involved entities.

8. Registration authority (RA): a specialized entity that registers private and public keys for each participant entity and keeps them secure in its own database. It also binds the keys to the concerted party and leaves no room for the forging of keys.
9. Judge: an entity responsible for verification purposes to submit evidence of unauthorized copies and to ensure authentication and intellectual properties.
10. Local anonymous generator: a type of generator for anonymously generating keys based on a specific input, which can be considered part of the WSP.
11. Local watermark generator: a type of watermark generator that uses a watermark algorithm.

3.2 Notations

The following notations have been used in our proposed scheme:

- $X \oplus W$: The watermarked copy of digital content X The binary operator $\oplus$ denotes watermark insertion operation, and W, the inserted watermark.
- H(R): Hash function for web user request.
- H(K): Hash function for the user public key.
- PK_i ,SK_i: A public-private key pair for i entity.
- (PK_i^* ,SK_i^*): A pair of generated anonymous keys for i entity.
- $E_{PKi}(m)$: Encryption of message m using i public key.
- $D_{PRi}(m')$: Decryption of message m' using i private key.
- H(T): Hashing process of timestamp
- W_i: Watermark associated with i entity.

3.3 Main Operation of the Scheme

1. Fig. 1 shows the first interaction will be completed between the web user and the CP, which is the website that provides services. Each of the CPs and web users must have a pair of keys, (PK_{CP}, SK_{CP}) and (PK_u, SK_u), respectively, depending on the RSA cryptosystem from homomorphism PKI [8], [10]. These generated keys will be used later to generate a pair of anonymous keys (PK^*_{CP}, SK^*_{CP}). Note that all messages of transmission are carried over the anonymizer (intermediary) entity to assure secure message transmission.

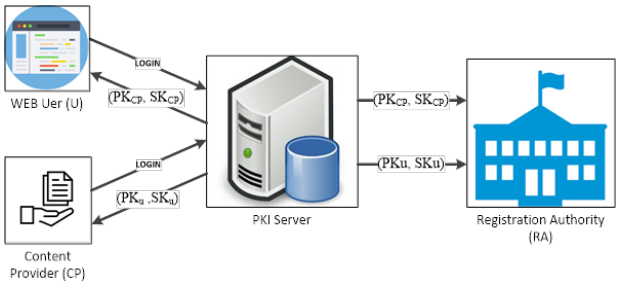


Fig. 1 The interaction between the web user and the CP

2. The web user will send a request message to the CP through a server, ($E_{PK^*U}(W_U)$,PK^*_U), and as a CP receives this request message, it will check its validity using a zero knowledge proof theory, and as sensitive information is required to be higher priority than other information, the CP will contact the WCA to obtain the watermark certificate for the watermarking operation and compute the W_{CP} by hashing the web user request and public key, H(R) and H(K), respectively, [38] to get W_{CP}, as in eq. 2:

$$W_{CP} = H(R) + H(K) \quad (2)$$

Additionally, a random sequence function, F_q, will be generated.

3. At the time W_{CP} is generated, the CP will also contact a CA to obtain its own general certificate based on a digital signature.
   - The CP will encrypt the W_{CP} using PK_{CP}, as in eq. 3:

$$E_{PKCP}(W_{CP}) = Enc(W_{CP})_{PKCP} \quad (3)$$

   - It sends the encrypted watermark, $E_{PKCP}(W_{CP})$, along with the CP public key, (PK_{CP}), to the CA for a digital signature.
   - The CA hashes the encrypted watermark and the CP public key and timestamp to obtain the $H(E_{PKCP}(W_{CP}), PK_{CP}, T_1)$,
     Where T_1 is a timestamp for the transaction that can solve any dispute.
   - A tuple, T_{CA}, is formed by combining the above information and timestamp T_1.
   - The tuple, T_{CA}, is hashed to obtain $H(T_{CA})$, as in eq. 4:

$$T_{CA}=\{ H(E_{PKCP}(W_{CP}), PK_{CP}, T_1), T_1\} \quad (4)$$

   - A digital signature, DS_{CA}, is obtained by encrypting $H(T_{CA})$ with the CA private key, (CA_{PR}), and then with the CP public key, as in eq.5:

$$DS_{CA}(T_{CA})=E(PK_{CP}(PR_{CA}(H(T_{CA})) \quad (5)$$

- The CA then sends the certificate to the CP, as in eq. 6:

$Cert_{CP}$ ={TCA,DSCA(TCA)} (6)

- The CP verifies the certificate by decrypting it with the CA public key and with its own private key to obtain $H(T_{CA})$.
- CP hashes T_{CA} to obtain $H_1(T_{CA})$. If $H(T_{CA})= H_1(T_{CA})$, it will be verified by the $Cert_{CP}$, which has been generated by the CA and has not been tampered with.
- The CP keeps the generated certificated in its own database, and a copy for the $Cert_{CP}$ will be kept in the CA database for verification purposes by any entity.

4. The CP will send the generated watermark certificate to the judge for verifying purposes as this certificate will be used as sensitive information for the watermarking operation. After verification, the CP encrypts the $E_{PK^*U}(W_U)$, W_{CP} and F_q using PK_{CP},PK^*_U and then sends the $E_{PKCP}(E_{PK^*U}(W_U))$, $E_{PKCP}(E(PK^*_U(W_{CP}))$, and $E_{PKCP}(E_{PK^*U}(F_q))$ with the watermarking generated certificate to the WSP to continue the dual watermarking process.
   As the WSP receives the CP message, it will confirm the doubly encrypted message and perform the following:
   (1) $E_{PKCP}(E_{PK^*U}(W_{CP})) \oplus E_{PKCP}(E_{PK^*U}(W_U))= E_{PKCP}(E_{PK^*U}(W_{CP} \oplus W_U)= E_{PKCP}(E_{PK^*U}(W_{CPU}))= E_{PKCP}(E_{PK^*U}(W_{CPU})) \oplus E_{PKCP}(E_{PK^*U}(Fq))= E_{PKCP}(E_{PK^*U}(W_{CPU} \oplus Fq))= E_{PKCP}(E_{PK^*U}(Fq(W_{CPU})))$
   (2) Applying a dual watermarking scheme based on threshold cryptography [39] for the proceeded webpage content.
5. The WSP sends the $E_{PKCP}(E_{PK^*U}(Fq(W_{CPU})))$ with a dual watermark webpage to the judge for verification purposes. As the judge receives the WSP message, it will verify it using zero knowledge proof, and as it becomes valid, it will be forwarded to the CP once more.
6. After judge verification, the CP will decrypt the $E_{PKCP}(E_{PK^*U}(F_q(W_{CPU}))$ using SK_{CP} to obtain the $E_{PK^*U}(F_q(W_{CPU}))$ and then the $E_{PK^*U}(F_q(W_{CPU})) \oplus E_{PK^*U}(X)$.
7. Finally, it sends the $E_{PK^*U}(F_q(W_{CPU})) \oplus X$) to the web user, who can decrypt it using SK^*_U and obtain the associated digital content, $F_q(W_{CPU}) \oplus X$.

4. Implementation

This section concerns the scheme implementation. First, the authors use modelsim SE 6.0 for watermarking and the PKI encryption process held by the WSP. Based on the logic field, the encoder is used for watermark embedding for the images associated with a website as strong evidence for CP authentication. Sensitive information associated with a webpage will have higher priority compared with other information that the CP may provide, in which a dual watermarking will be performed based on threshold cryptography (HTML code) [39].
The scheme depends on the dual watermarking based on threshold cryptography, and thus the generated watermark will be imbedded into the tags of the source code of webpages (HTML) by moving along vertically and horizontally in a layer. To a certain extent, embedding the watermark in both a vertical and horizontal direction for double watermark segments in the layers can be viewed as a dual digital watermarking scheme.
In the instance of watermark slicing in 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 or inconsistent with the content, and tampering is easily covered [39]. The main **distinguishing factor** from [39] is that:

- Embedding the double quoted parts of the HTML tags will be omitted. The idea behind omitting is to save time for the watermark generation process. Consequently, during the detection or recovery process, it will be ignored.
- Embedding the watermark into the tags of the HTML code will make use of case-insensitive HTML tags. Then, if a certain bit of the watermark is 0, the corresponding character in the tags will then be converted into lowercase, and otherwise to uppercase [33], in the watermark recovery process.
- At each layer, the first authentication code from a line of digital watermarking and the second authentication code from a column of digital watermarking will be combined within a layer. Thus, the entire digital watermark would be embedded into the HTML tag.

As the scheme will be implemented in the proposed way, the authors guarantee that the size of the document will not increase, and the function associated with a web files will not be affected.
What performed by WSP from hashing, double encryption under PKI and dual watermarking is implemented depend on the logic field (Encoder for watermark embedding and decoder for watermark extraction). The watermark embedded for web images

which may be a sign or a web quran page designed and implemented as an image.

4.1 The Watermark Embedded Operation

The entire 8-bit grayscale image is divided into blocks of 16x8 (=128) pixels. For each of these image blocks the watermark insertion is carried out sequentially.
Main operations carried out by the following flags:

- "reg_enable" that load one pixel at a time
- The "reg_lsb" and "reg_msb." Will be used to hold the 128 MSB's of the pixels that are going to be embedded with the watermark.
- "msb_enable" goes high when "reg_msb" loads data goes high. This flag correspond to the signal "msg_in_valid" of the Hasher.
- "msg_out_valid" signal goes high indicating completion of the hash operation.

The watermark embedded image block is then stored back at the same location and the whole process begins again. Fig. 2 shows the implementation of the whole process.

4.2 The Watermark Extraction Operation

The entire 8-bit grayscale image is divided into blocks of 16x8 (=128) pixels. For each of these image blocks the watermark extraction and detection is carried out sequentially. Same flags that used in encoding but the main distinguish is that, working in extracting (decoding). Noted that, the extracted watermark is then compared with the watermark bitstream originally embedded by XORing the 2 bit streams. The resultant bitstream represents the comparison result. A stream of all zeroes indicates a perfect match and correct detection. Once the detection is done the signal "decout_ready" goes high indicating the decoder is ready to decode the next block of image data.
The whole process begins again with the loading of the next block of image data onto the register file. Fig. 3 shows the implementation of the whole process.

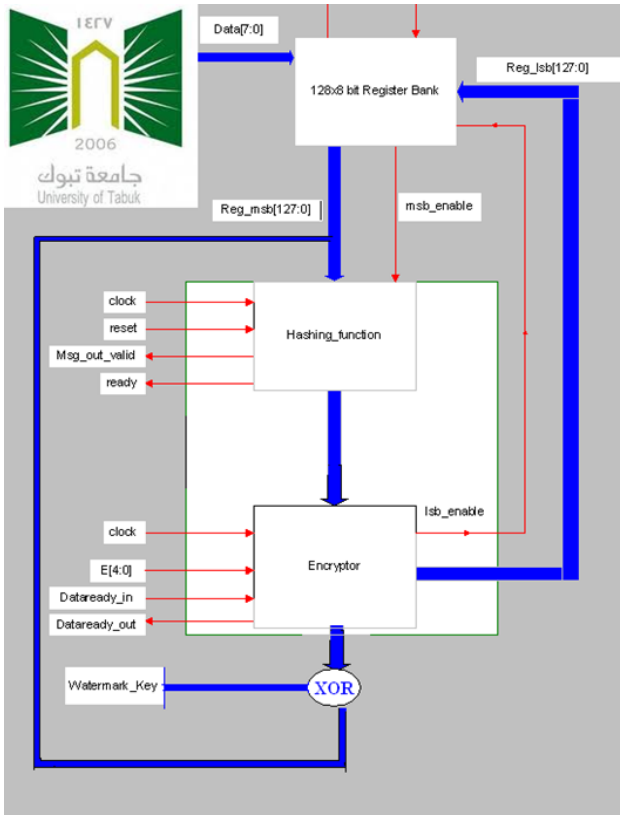


Fig. 2 Encoder Block Diagram

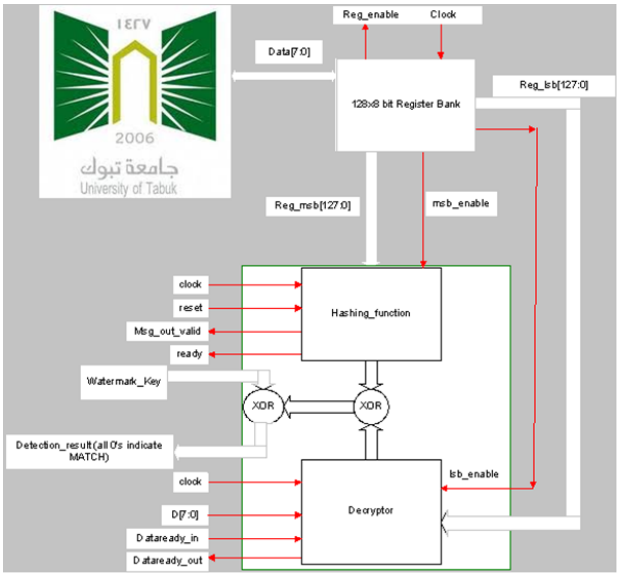


Fig. 3 Decoder Block Diagram

The modules for the Encoder and the Decoder were written in Verilog and their functional verification was done using MODELSIM 6.0a.

The proposed scheme has been evaluated in terms of the following:

- **Invisibility**: no clear visual difference between the original webpage and the watermarked page after applying the proposed scheme.
- **Robustness**: Specialized software is used to test and detect pre- and post-watermarking at the pixel level after damaging the first sentence to verify the robustness of the watermark. Fig. 4, 5, and 6 shows the WSC, SCC, and RP detect nothing if the first sentence of the document has been damaged; while fig. 7 shows the modified DWTC is tamper proof if the document has been damaged.

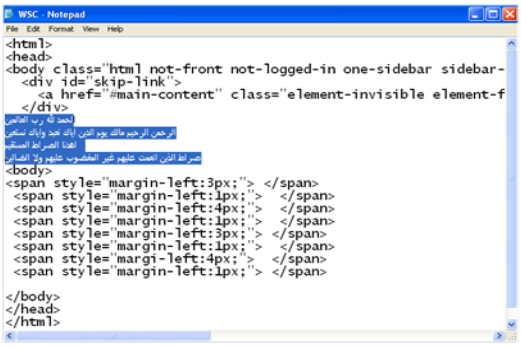


Fig. 4 WSC watermark detection after tamper webpage

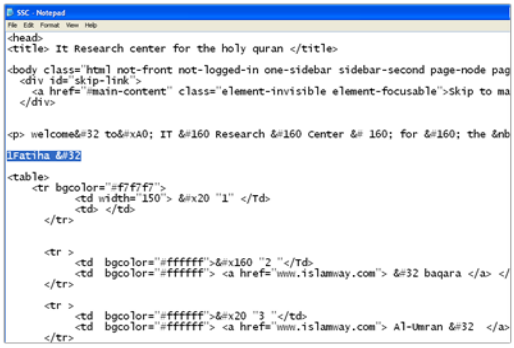


Fig. 5 SSC watermark detection after tamper webpage

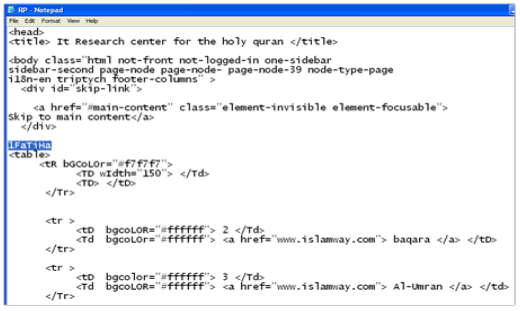


Fig. 6 RP watermark detection after tamper webpage

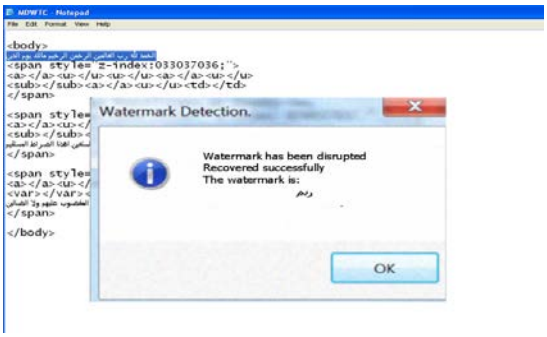


Fig. 7 MDWTC watermark detection after tamper webpage

- **Efficiency:** Fig. 8 shows the result of the proposed scheme based on the result for RP, SSC, and WSC for the watermark embedding time, as in [39]. The result shows a strong improvement in the watermark embedding time in comparison with others scheme, especially when the file size is larger.

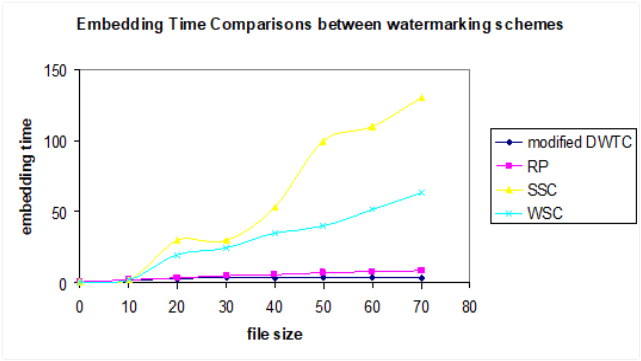


Fig. 8 Embedding time among different watermarking schemes

5. Conclusion

An effective and secure watermarking protocol is proposed that encapsulates a flexible and convenient solution for CP authentication and integrity problems. The security of the proposed protocol is based on the security of the PKI and dual watermarking based on threshold cryptography. The proposed protocol exploits the existence of the trusted CA to solve collusion problems and to apply the idea of zero knowledge proof for verification purposes. The analysis results show the functional verification for encoder (watermark embedding), decoder (watermark extracting), encrypt (encryption), decryptor (decryption), and hashing. Additionally, the evaluation results are better for modified DWTC compared with other schemes (RP, WSC, and SSC).

Acknowledgments

This Project was funded by the Deanship of Scientific Research (DSR) at University of Tabuk, Tabuk, under grant no. S-0069-1439. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

References

[1] 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.

[2] 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.

[3] Katzenbeisser, Stefan. "On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking." Database and Expert Systems Applications, 2001. Proceedings. 12th International Workshop on. IEEE, 2001.

[4] Frattolillo, Franco. "Watermarking protocol for web context." IEEE Transactions on Information Forensics and Security 2.3 (2007): 350–363.

[5] Campidoglio, M., Franco Frattolillo, and Federica Landolfi. "The copyright protection problem: Challenges and suggestions." Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on. IEEE, 2009.

[6] Kirovski, Darko, Henrique Malvar, and Yacov Yacobi. "A dual watermark-fingerprint system." IEEE multimedia 11.3 (2004): 59–73.

[7] Zhao, Jian. "Applying digital watermarking techniques to online multimedia commerce." Proc. Int. Conf. on Imaging Science, Systems and Applications (CISSA'97). Vol. 7. 1997.

[8] Mazurczyk, Wojciech, and Zbigniew Kotulski. "Covert channel for improving VoIP security." Advances in Information Processing and Protection. Springer, Boston, MA, 2007. 271–280.

[9] Memon, Nasir, and Ping Wah Wong. "A buyer-seller watermarking protocol." IEEE Transactions on image processing 10.4 (2001): 643–649.

[10] Cheung, Shing-Chi, and Hanif Curreem. "Rights protection for digital contents redistribution over the Internet." Computer Software and Applications Conference, 2002. COMPSAC 2002. Proceedings. 26th Annual International. IEEE, 2002.

[11] Jun, J. M., et al. "Digital watermarking and practical distribution protocol for digital contents copyright protection." Proceedings of the WISA. 2000.

[12] Shilbayeh, Nidal F., and Adham Alshamary. "Digital Watermarking System based on Cascading Haar." Journal of Applied Sciences 10.19 (2010): 2168–2186.

[13] Kwok, Sai Ho, et al. "Integration of digital rights management into the Internet Open Trading Protocol." Decision Support Systems 34.4 (2003): 413–425.

[14] Honsinger, Chris. "Digital watermarking." Journal of Electronic Imaging 11.3 (2002): 414.

[15] Van Schyndel, Ron G., Andrew Z. Tirkel, and Charles F. Osborne. "A digital watermark." Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference. Vol. 2. IEEE, 1994.

[16] Tanaka, Kiyoshi, Yasuhiro Nakamura, and Kineo Matsui. "Embedding secret information into a dithered multi-level image." Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE. IEEE, 1990.

[17] Brassil, Jack T., et al. "Electronic marking and identification techniques to discourage document copying." IEEE Journal on Selected Areas in Communications 13.8 (1995): 1495–1504.

[18] Bender, Walter, et al. "Techniques for data hiding." IBM systems journal 35.3.4 (1996): 313–336.

[19] Smith, Joshua R., and Barrett O. Comiskey. "Modulation and information hiding in images." International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 1996.

[20] Agreste, Santa, et al. "An image adaptive, wavelet-based watermarking of digital images." Journal of Computational and Applied Mathematics 210.1-2 (2007): 13–21.

[21] Cox, Ingemar J., Joseph J. Kilian, and Talal G. Shamoon. "Secure spread spectrum watermarking for multimedia data." U.S. Patent No. 5,930,369. 27 Jul. 1999.

[22] Hartung, Frank H., and Bernd Girod. "Watermarking of MPEG-2 encoded video without decoding and reencoding." Multimedia Computing and Networking 1997. Vol. 3020. International Society for Optics and Photonics, 1997.

[23] Craver, Scott A., et al. "Can invisible watermarks resolve rightful ownerships?." Storage and Retrieval for Image and Video Databases V. Vol. 3022. International Society for Optics and Photonics, 1997.

[24] Bloom, Jeffrey A., et al. "Copy protection for DVD video." Proceedings of the IEEE 87.7 (1999): 1267–1276.

[25] Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia." IEEE transactions on image processing 6.12 (1997): 1673–1687.

[26] Furon, Teddy, and Pierre Duhamel. "An asymmetric watermarking method." IEEE Transactions on Signal Processing 51.4 (2003): 981–995.

[27] Eggers, Joachim J., Jonathan K. Su, and Bernd Girod. "Public key watermarking by eigenvectors of linear transforms." Signal Processing Conference, 2000 10th European. IEEE, 2000.

[28] Memon, Nasir, and Ping Wah Wong. "A buyer-seller watermarking protocol." IEEE Transactions on image processing 10.4 (2001): 643–649.

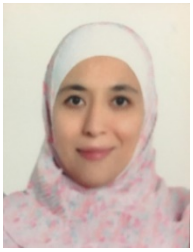
[29] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120–126.

[30] Johnson, Neil F., Zoran Duric, and Sushil Jajodia. "Recovery of watermarks from distorted

images." International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 1999.
[31] Morovati, Kamran, Sanjay Kadam, and Ali Ghorbani. "A network based document management model to prevent data extrusion." Computers & Security 59 (2016): 71–91.
[32] Birk, Dominik, Seán Gaines, and Christoph Wegener. "A framework for digital watermarking next generation media broadcasts." Axmedis 200845 (2008): 19.
[33] Jun, J. M., et al. "Digital watermarking and practical distribution protocol for digital contents copyright protection." Proceedings of the WISA. 2000.
[34] Housley, Russell, et al. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. No. RFC 3280. 2002.
[35] Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005.
[36] Cohen, Josh D., and Michael J. Fischer. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, 1985.
[37] He, Yong-Zhong, Chuan-Kun Wu, and Deng-Guo Feng. "Publicly verifiable zero-knowledge watermark detection." Ruan Jian Xue Bao(Journal of Software) 16.9 (2005): 1606–1616.
[38] Sverdlov, Alexander, Scott Dexter, and Ahmet M. Eskicioglu. "Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies." Signal Processing Conference, 2005 13th European. IEEE, 2005.
[39] Li, Daojing, and Bo Zhang. "DWTC: A dual watermarking scheme based on threshold cryptography for web document." Computer Application and System Modeling (ICCASM), 2010 International Conference on. Vol. 8. IEEE, 2010.
[40] Ambadekar, Sarita P., Jayshree Jain, and Jayshree Khanapuri. "Digital Image Watermarking Through Encryption and DWT for Copyright Protection." Recent Trends in Signal and Image Processing. Springer, Singapore, 2019. 187–195.

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.



Miss. Reem A. Al-Saidi was born in Jordan on 8th Nov 1988. She received her master degree from Middle East University, Jordan with honor degree in 2011 and her bachelor's degree from the University of Jordan, Jordan in 2010.

From 2013 till now, she works as a Teaching and Research Assistant and holding the responsibility for lab supervision and practical teaching lessons at the University Of Jordan, King Abdallah Second School for information Technology, Computer Science Department. Her research interest includes Cryptography and Information security, E voting system security issues, Human Computer Interactions and System Usability; Image processing, Watermarking Techniques and Steganography.