Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Watermarking implementation on digital images and electronic signatures

Ahmad Abdul Qadir AlRababah *

Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Rabigh 21911, Saudi Arabia

ARTICLE INFO

Article history:
Received 19 June 2017
Received in revised form
7 September 2017
Accepted 11 September 2017

Keywords:
Digital images
Digital signature
Digital steganography
Digital watermarks

ABSTRACT

For successful business, information technology is becoming increasingly important. After all, with the help of its information system, each company organizes all internal processes, interacts with external partners, contractors and customers, government agencies. About the provision of information security a lot has already been written, but in this article the authors pay attention to one of the methods that can be used to protect against committing malicious acts directed against the company from within. The proposed method perfectly copes with the internal threat, however, as well as with the external one. The main task in this manuscript is to create a method for countering counterfeits of digital photos, and describes the algorithm for protecting the image.

1. Introduction

Embedding in digital photos of invisible Tags, such as character sequences or graphic images, is one of the widespread ways to protect the information content of these photos. Such marks were called digital watermarks, in analogy with the widely known method protection of securities from counterfeits (Mansouri et al., 2010). The method of protection of graphic information by means is a part of the digital steganography, the science of the inconspicuous concealment of some data in others (AlRababah, 2017a; AlRababah, 2015).

As the statistics show, more than 80% of incidents with the information system are initiated from within the corporate network - violations are committed by their own employees. Ensuring the safety and the permanent operation of the information system is one of the priorities of any company for survival in the acute competitive struggle (Wu et al., 2009; AlRababah, 2017b).

2. Materials and methods

Joint protection by digital signature and watermarking**:** A watermark is one of the most popular ways to put property rights on a photo, either by text or logo. It is very practical and protects your photos from theft, especially if you are a designer or photographer and want to sell your photos on the Internet or have a website to host photos. To create a professional signature on the image makes it difficult for anyone who tried to remove the signature and image ratios for himself, and to do so easily you in one of the services available on the Internet provided by several sites in order to put the watermark on the image for free.

As a result of the widespread spread of electronic transactions, the shift from paper transactions to electronic transactions more liquid and less complex but the challenge lies in the implementation of these transactions in terms of authentication and insurance, and can be considered to digital signature technology as a mechanism to maintain safety and security in e-transactions.

As the Internet continues to share information and communication, security concerns are becoming more critical. Digital signature will work to improve our transactions and communications in a better way with high safety (Langelaar and Lagendijk, 2001; AlRababah and Biswas, 2008)**.** It is noted that when conducting transactions electronically, there is no way to confirm the identity of the sender poisoning, and hence the possibility of using digital signatures for electronic authentication on the source of messages transactions, the electronic signature confirms the true identity of the sender to keep safe data, since the modification of messages or transactions after termination is out of the question, which constitutes a source of strength and excellence electronic signatures as an effective solution for authentication and authentication**.**

In view of the security and integrity of electronic transactions and the extent of damage and embarrassment that may occur in many sectors governmental and private transactions when dealing

* Corresponding Author.
Email Address: aahmad13@kau.edu.sa
https://doi.org/10.21833/ijaas.2017.010.022

with piracy or unauthorized use, the availability of signatures affordable and convenient for all applications and businesses has become a necessity, as there continued to exert pressure to protect the business sector in general from global activities and poor use, the same is true for all business sectors, regardless of sector size to improve the integrity of e-transactions for all sectors and effectively implement them to achieve blind economic returns.

For example, e-banking requires a high level of security so that it can build customer confidence when used but unfortunately, bank fraud is on the rise, although many banks are developed the access mechanism for banking services, such as confirming the entry of a secret number sent through mobile or other handsets a number of international banks are therefore seeking to adopt existing e-signature mechanisms biometric properties to increase the safety of access to electronic banking transactions.

The use of electronic signatures will also help reduce the reliance on paper usage in all our transactions in the same context; they will work towards geodesy aimed at promoting green environment, using electronic signatures. To perform such tasks, a method of reversible data hiding was invented (Aljumah and Ahamad, 2016).

Digital signature technique

A two-key mathematical formula is made by means of a private Key, which know only the sender used to encrypt the data and the second a public key, used to decrypt the message and known to the recipient or to a trusted recipient of the login needed. If one wants to create a value for a fee, a digital file is digitally signed, with special software available at the site by applying the physical data sensor function, you then encrypt the value using the sender's private key, attach the signature (value after the encryption) with the message.

Finally, the receiver used the public key and the private key is used by a sender to decrypt the signature code, the successful decryption of the signature code, means that the sender has already signed the message, and as a second step, future software calculates the result of a new message using the same interface function that used in the digital signature filter, to get a value of the signature has been matched (Sun et al., 2009; AlRababah, 2016).

The essence of this method is to integrate invisible control data containing the information about the part to be changed into the file to be protected. When extracting data from a file, for example, a picture, it can be brought to its original appearance (Wang et al., 2012; AlRababah, 2015; Ling et al., 2004a; 2004b). In addition, you can always make sure that any changes have been made to the picture after the data has been inserted. But this may not be enough.

In addition, as is known, the digital signature, when applied as a single security link does not always provide a 100% security guarantee. The author suggest the following solution, combining the use of digital signatures and watermarking, namely: sign the entire container with embedded watermarking electronic digital signature on the private key of an authorized employee. Obtain the received signature for storage by the certifying center, which also stores public keys with employee certificates. The latter option is especially relevant for the organization of mutual exchange of legally significant electronic documents between various organizations (Chen and Lin, 2006; Lu and Liao, 2001).

In the protected file, the digital timestamps of the file signing time can additionally be embedded. This will allow organizing intercorporate control over the use of the document management system. Every legal user can verify the authenticity and permanence of an electronic document with the help of a public key from the certifying center.

The digital watermark hidden in the file is a guarantee that even if an attacker signs a file on his behalf, the results of checking his signature and the digital watermarking do not coincide and a violation can be established. Digital watermarking acts as an additional level of protection, which is sometimes difficult to even detect (AlRababah, 2017b; Setyawan and Lagendijk, 2001).

Certificates for public keys of a signature can be issued and stored by certification centers, for which a similar function is fixed in accordance with the law of the country "On digital electronic signature". The certificate confirms that the public key does belong to a certain person. In addition, on the server of the certifying center it is possible to organize the storage of digital signatures of the authors of all created documents. The mechanism of electronic digital signature is built on the principles of two-key asymmetric cryptography (Mansouri et al., 2010; Chen and Lin, 2006).

Simultaneous use of several technical protection measures – Digital Signature, Digital Watermarking and timestamp - will significantly complicate and increase the cost of malicious actions, such as changing the container, substituting authorship, etc. Since the security tools are used independently, overcoming one of them does not allow an attacker to change the file for their own purposes, without notice and with impunity (Wu et al., 2009; Ling et al., 2004a; 2004b; AlRababah, 2016).

Another cryptographic vulnerability is the selection of changes in the file so that the digital signature remains the corresponding modified file.

The possibility of this decrease exponentially with increasing the length of the key used and the length of the hash value (a unidirectional cryptographic function that is used in the algorithms for generating digital signatures and in digital signatures verification algorithms (Redwan and Kim, 2008; Sharma et al., 2012).

Agree that it is extremely difficult for even a computer to scan billions of variants of a large file, since it is necessary to produce cryptographic calculations that require a lot of time and processor resources. And if it still can be done, then in the file

still remain inconspicuous digital signs with information about the true author of the signature (Wang et al., 2012; Sun et al., 2009).

Protection from internal violators

Let everyone know about the availability of electronic digital signatures. If you do not notify staff about the use of the method of embedding digital watermarks in all electronic documents

of the information system, if a successful attempt to forge a signature or make unauthorized changes to the document, the digital watermarking check reveals a malicious effect. For these actions (an attempt to deceive the digital signature system), one can judge the intentionality of the act committed by the offender. The combination of protection of the document with the help of digital signatures and digital watermarking will make it possible to establish the culprit. Even if the user had the right at his level to use his key to generate a digital signature for an unchanged file, the digital watermarking check will report a malicious act, because their intruder cannot change. The reliability of detecting an attacker is increased if the digital watermarking contains the identifiers of the users who modified or created the file. Of course, if an electronic document from outside is entered into the document management system; it will be immediately revealed by the absence of any digital labels in the file (Ling et al., 2004a; 2004b; AlRababah and Biswas, 2008).

3. Experiments

Consider the situation when the protection of digital photography is performed for the purpose of proving it illegal use or possible falsification. In this case, the original image can be subjected to a number of external influences, which include noise, cutting edges images, framing, filtering, rotations, changing the digital format, loss compression and scaling. Also, any fragments of the protected photo can be added or conversely deleted. Some of these impacts, such as noisy or filtering, are directed directly at removing or damaging possible embedded marks; other example, cropping and scaling, are aimed at preparing the image for its use (Arunmozhi and Venkataramani, 2011).

A method that allows guaranteeing the stability of embedded elements in the image, affecting noise, filtering image, and also indicating the change of its various fragments, is assumed that when attempt to replace the violator with fragments of the marked image by others after the attraction procedure of foreign objects will become noticeable and facilitates the proof of the falsification of digitalization.

From existing digital image formats for storing full color photos, The JPEG and JPEG2000 formats are suitable, because the images saved in these formats have high quality indicators for relatively small file sizes. Lack of

these formats is that to reduce the size of graphics files, an algorithm is used to compress them with losses, which means that some of the information will be irreversibly lost if you save such images, and, therefore, there is a possibility of distortion or loss.

To increase the robustness of embedded attachments to compression or scaling graphics files in stegoalgorithms, try to apply the same transformations as in the compression algorithms of these files. For JPEG format, this algorithm is a discrete cosine transformation.

The JPEG2000 graphic format has several advantages over the JPEG format. This is the best Image quality with equal compression, optimization of encoding quality, and lossless compression capability. Therefore, when choosing the format for saving digital photos, it is better prefer a more modern JPEG2000.

The developed algorithm for embedding information should be based on the wavelet transform, since in this case the digital watermarks will be resistant to compression Images.

In general, for the stability of the digital watermarks to various distortions in photography, it is necessary to repeatedly embedded in it, which means that the size of embedded labels should be much smaller than the size of the protected image.

Previously, the existing method of embedding digital watermarks of images in JPEG2000 format using the wavelet transform by marking the most significant parts of the image with taking into account the peculiarities of human perception. Such a method is quite effective for evidence of the authenticity of digital photography, since the information so embedded it is difficult to damage or remove without degrading the visual qualities of the image itself. However, this method is not entirely suitable for proving the fact of cropping the original image, as well as removing or replacing its significant parts.

When developing a new method, it is necessary to take into account the advantages of the above mentioned existing one, i.e. the embeddable digital watermarks must be resistant to its filtering and compression, and the

marking of the image areas should be carried out in such a way that when the procedure for extracting images, the digital watermarks must check for authenticating the image, whether it was truncated, and whether its parts were removed or replaced.

4. Results and discussions

The following algorithm can be used to achieve this goal:

- The original image, which can be represented as a matrix $f(n, m)$, is divided into the same blocks a_{ij} the size 64 x 64 pixels (Fig. 1).
- The algorithm for the arrangement of the digital watermarks, which is a matrix w (m, n) 4 x 4 pixels in size, is chosen in these blocks. It is advisable to build in each block of 4 digital watermarks, deviating from the edge by at least 3 pixels, but

placing them asymmetrically relative to this block (Fig. 2).

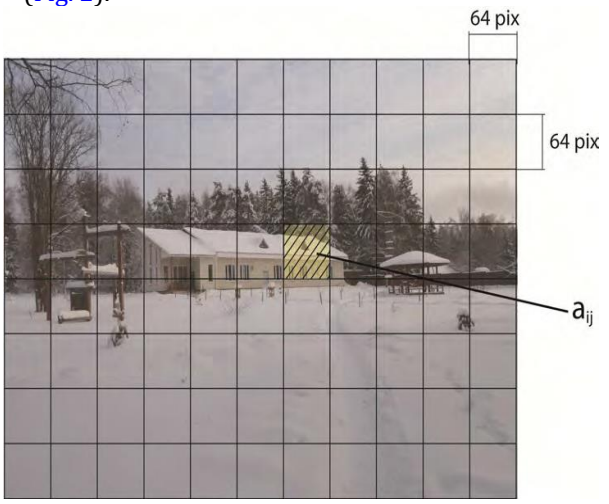

Fig. 1: The image is divided into blocks

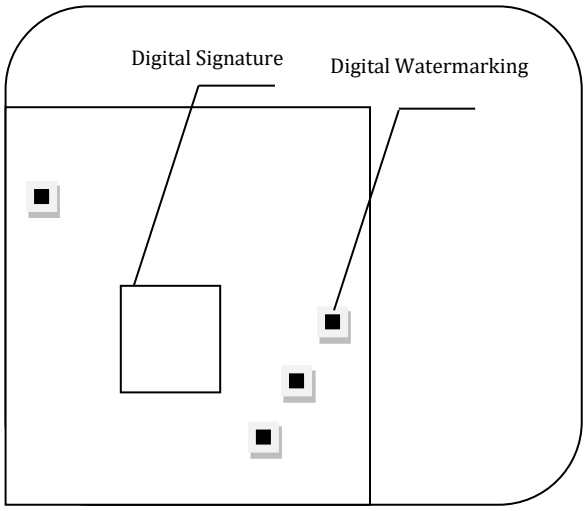

Fig. 2: An example of embedding a digital watermarks and electronically digital signature in image blocks

The next steps of the developed algorithm for the protection of the photo image are associated with embedding in an image of digital watermarks that acts as an electronic digital signature. Unlike the rest of the digital watermarks, embedded in the blocks of digital signatures must be different and characterize such properties of the image as, for example, its brightness, contrast, color filtering and low-pass filtering, as well as information about the image in general (the size of the image, the number of blocks in it) and adjacent blocks.

Each digital signature must be built clearly in the middle of each block, without trying to choose the most successful sites for robustness. This is due to the fact that the full or partial absence of these central marks in the monitored image will indicate that this photo was exposed to any influences. In this case, other built-in digital watermarks should be as robust as possible to attack, so that you can talk about copyright infringement rights to this image.

The difference between the built-in digital signatures from each other is necessary to determine the application to the image framing procedure. Let's return to the algorithm.

- An algorithm is chosen for applying various digital signatures to the blocks (Fig. 3).

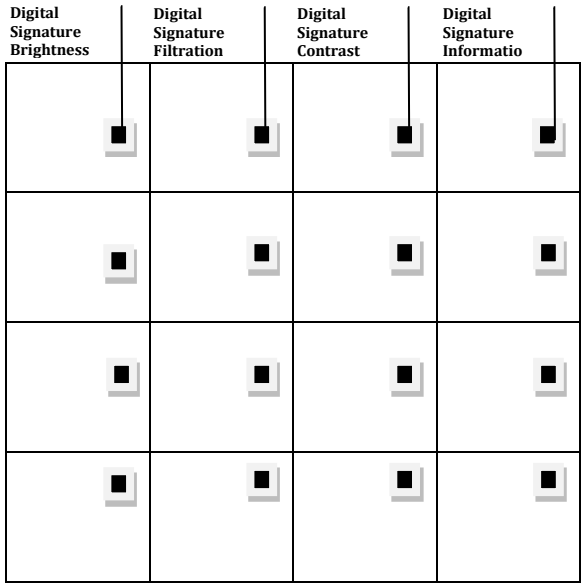

Fig. 3: An example of an algorithm for depositing a digital signature in an image block

- Digital signatures are made depending on their purpose.
- Digital signatures are built into image blocks in accordance with the chosen algorithm.
- Digital signatures of each block are adjusted depending on neighboring locks.

In the next step, the image undergoes a reverse wavelet transformation, resulting in it turns out to be marked. Due to the division of the original photo image into blocks, the unbalanced marking of the digital watermarks blocks and the presence in the center of each digital signatures block located according to the chosen algorithm, when verifying the authenticity of the image, it is possible to determine whether it has been truncated, filtered or otherwise attacked.

5. Conclusion

The proposed system has sufficient resistance to possible attacks, since the use of weaknesses in this case is costly and resource-intensive. This allows us to recommend the proposed method as a technical measure to protect electronic documents from both internal and external violators. Implementation in the protected picture has met two conflicting criteria of robustness (resistance to various external and secrecy, ensuring the least distortion of the image in comparison with original). To verify the copyrights to a digital image, extract built-in information, which, with insufficient robustness may become impossible for attacks.

Acknowledgment

I thank King Abdulaziz University- KSA for providing me with needed resources for carrying out this work.

References

Aljumah A and Ahamad T (2016). A novel approach for detecting DDoS using artificial neural networks. International Journal of Computer Science and Network Security, 16(12): 132-138.

AlRababah AA (2015). Lempel-Ziv implementation for a compression system model with sliding window buffer. International Journal of Advanced Computer Science and Applications, 6(10): 101-104.

AlRababah AA (2016). Embedded architecture for object tracking using Kalman filter. Journal of Computer Science, 12(5): 241-245

AlRababah AA (2017a). On the associative memory utilization in English- Arabic natural language processing. International Journal of Advanced and Applied Sciences, 4(8): 14-18.

AlRababah AA (2017b). A new model of information systems efficiency based on key performance indicator (KPI). International Journal of Advanced Computer Science and Applications, 8(3): 80-83.

AlRababah AA and Biswas R (2008). Rough vague sets in an approximation space. International Journal of Computational Cognition, 6 (4): 60-63.

Arunmozhi SA and Venkataramani Y (2011). A new defense scheme against DDoS attack in mobile Ad Hoc networks. In: Meghanathan N, Kaushik BK, and Nagamalai D (Eds.), Advanced Computing, CCSIT 2011. Communications in Computer and Information Science: 133. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-17881-8_21

Chen PY and Lin HJ (2006). A DWT based approach for image steganography. International Journal of Applied Science and Engineering, 4(3): 275-290.

Langelaar GC and Lagendijk RL (2001). Optimal differential energy watermarking of DCT encoded images and video. IEEE Transactions on Image Processing, 10(1): 148-158.

Ling H, Lu Z, and Zou F (2004a). New real-time watermarking algorithm for compressed video in VLC domain. In the International Conference on Image Processing, IEEE, Singapore, Singapore, 4: 2171-2174. https://doi.org/10.1109/ICIP.2004.1421526

Ling H, Lu Z, and Zou F (2004b). Improved differential energy watermarking (IDEW) algorithm for DCT encoded image and video. In the 7th International Conference on Signal Processing, IEEE, Beijing, China, 3: 2326-2329. https://doi.org/10.1109/ICOSP.2004.1442246

Lu CS and Liao HYM (2001). Video object-based watermarking: a rotation and flipping resilient scheme. In the International Conference on Image Processing, IEEE, Thessaloniki, Greece, 2: 483-486. https://doi.org/10.1109/ICIP.2001.958533

Mansouri A, Aznaveh AM, Torkamani-Azar F, and Kurugollu F (2010). A low complexity video watermarking in H. 264 compressed domain. IEEE Transactions on Information Forensics and Security, 5(4): 649-657.

Redwan H and Kim KH (2008). Survey of security requirements, attacks and network integration in wireless mesh networks. In the New Technologies, Mobility and Security, IEEE, Tangier, Morocco: 1-5. https://doi.org/10.1109/NTMS.2008.ECP.94

Setyawan I and Lagendijk RL (2001). Low-bit-rate video watermarking using temporally extended differential energy watermarking (DEW) algorithm. In: Wong P and Delp EJ (Eds.), Security and watermarking of multimedia contents: 73-84. Society of Photo-Optical Instrumentation Engineers (SPIE), Bellingham, Washington, USA.

Sharma P, Sharma N, and Singh R (2012). A secure intrusion detection system against DDOS attack in wireless mobile Ad-hoc network. International Journal of Computer Applications, 41(21): 16-21.

Sun T, Jiang X, Shi S, Lin Z, and Fu G (2009). A Novel Self-adaptation differential energy video watermarking scheme in copyright protection. Journal of Multimedia, 4(3):153-160.

Wang L, Ling H, and Lu Z (2012). Real-time compressed-domain video watermarking resistance to geometric distortions. IEEE Multi Media, 19(1): 70-79.

Wu D, Kong W, Yang B, and Niu X (2009). A fast SVD based video watermarking algorithm compatible with MPEG2 Standard. Soft Computing-A Fusion of Foundations, Methodologies and Applications, 13(4): 375-382.