Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

A new approach for watermarking products with the buyer's name to prevent fraud

Saad Abdual Azize abdual Rahman and Sana Ahmed Kadhim *

Al_Ma'moon University College, Computer science dept, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2021, 08(02), 076–081

Publication history: Received on 26 July 2021; revised on 29 August 2021; accepted on 31 August 2021

Article DOI: https://doi.org/10.30574/gjeta.2021.8.2.0132

Abstract

Due to the fast development in E-commerce and E-payment fraud has become one of the most serious problems. Therefore, most of the international companies invented their own watermark so as to maintain these companies to aqueous brands from forgery and tried to find different ways to preserve it. In this paper a proposed method was suggested that aims to develop a code name for the buyer using one of the watermarking techniques to allow the buyer to certify the source of purchases before payment.

Keywords: SRSA; Move – to – Front coding; Zigzag; Watermark

1. Introduction

The fast advancement of the Internet and the computerized data unrest brought on critical changes in the worldwide society, extending from the impact on the world economy to the way individuals these days convey. Broadband correspondence systems and mixed media information accessible in an advanced configuration (pictures, sound, video) opened numerous difficulties and open doors for development [1].

All together for a watermark to be valuable, it must be perceptually undetectable and vigorous against any conceivable assault and picture preparing by the individuals who look to corsair the material [2, 3].

Computerized watermark is a code that is inserted inside some honest looking spread information. Commonly, this data is required to be powerful against any purposeful evacuation by noxious gatherings. Rather than cryptography, where the presence however not the importance of the data is known, watermarking means to cover up completely the presence of the data. Watermarking has existed following around the thirteenth century and the past watermarks were utilized on the papers to distinguish the plant which made them [4].

2. Watermarking

In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image [6],[7]. Tirkel et al [8] were one of the first used techniques for image watermarking. Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications. The algorithm proposed by Kurah and McHugh's [9] to embed in the LSB and it was known as image downgrading [10].

* Corresponding author: Sana Ahmed Kadhim
Al_Ma'moon University College, Computer science dept, Baghdad, Iraq.

Digital watermarking is the process of embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm (Megías, Serra-Ruiz, & Fallahpour, 2010).

3. Move –to – front coding

Suppose we are given a sequence of symbols as before, with each symbol coming from an alphabet {A1, . . . , AN }. The move-to-front algorithm maintains a list of the N symbols in the alphabet. For each symbol in the sequence, it encodes the position of this symbol in the list, and then modifies the list by moving the symbol to the front of the list.[8]

3.1. RSA

One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adelman at MIT and first published in 1978.

RSA is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. Encryption and decryption are of the following form, for some plain text block M and cipher text block C[10] .

3.2. SRSA algorithm

KEY GENERATION

1-Select p1, p2……pn prime number

2-Calculate n = p1 * p2……..*pn

3-Calculate Φ (n) = (p1-1) (p2-1)……..(pn-1)

4-Select integer e gcd (Φ (n), e)=1; 1 < e < Φ (n)

5-Calculate d d ≡ e -1 mod Φ (n)

6-Public Key KU = {e, n}

7-Private Key KR = {d, n}

ENCRYPTION

8-Plain text =M M < n

9-Cipher text =C C = M e (mod n)

DECRYPTION

Plain text = M = C d (mod n)

3.3. Zigzag method

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext.

The rail fence cipher (also called a zigzag cipher) is a form of classical transposition cipher. It derives its name from the manner in which encryption is performed.

In the rail fence cipher, the plaintext is written downwards diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached, down again when the top rail is reached, and so on until the whole plaintext is written out. The cipher text is then read off in rows.

3.4. The proposed method

The proposed method has the following steps:

3.4.1. Embedding method

- taken the name of owner.
- using Move –to – front coding
- using SRSA development to encryption the output of 2.
- using zigzag to embedding the data in the water mark.

3.4.2. Extracting method

- Using zigzag to extract the data from watermark.
- Apply the SRAS to decrypted the data.
- Using Move –to – front decoding the data to get the message.

To explain the proposed method, an example will be explained in details the steps:
Suppose the buyer's name is "Salem saad", then by using MTF method we obtain the following table.

Table 1 Applying MTF method

Scanned letter	Numbers	English letter
S	19	Abcdefghijklmnopqrst
Sa	19,2	Sabcdefghijklmnopqrt
Sal	19,2,13	as bcdefghijklmnopqrst
Sale	19,12,13,7	las bcdefghijkmnopqrst
Salem	19,12,13,7,14	elas bcdfghijkmnopqrst
Salems	19,12,13,7,14,5	melas bcdfghijknopqrst
Salemsa	19,12,13,7,14,5,5	smela bcdfghijknopqrst
Salemsaa	19,12,13,7,14,5,5,1	asmel bcdfghijknopqrst
Salemsaad	19,12,13,7,14,5,5,1,8	dasmel bcfghijknopqrst

The result from the previous table will be: o/p = 19,12,13,7,14,5,5,1,8

3.5. Applying RSA

Plain text =19,12,13,7,14,5,5,1,8

Cipher text = 94,3,97,28,14,80,80,1,92

the implementation of the process is shown with figures 1,2 and 3.

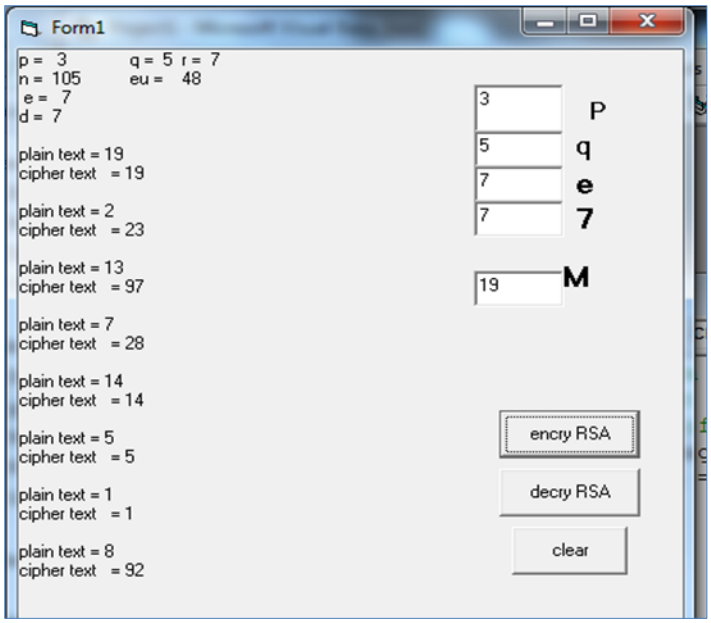

Figure 1 Implementation of RSA

Embedded the cipher text in the watermark as shown in figure 2 below:

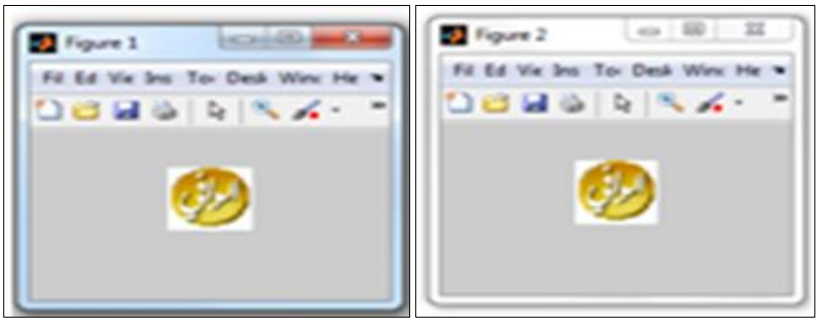

Figure 2 Implementation of Embedding process

Use the zigzag method to embed the cipher text in watermarking, showing the data before and after embed.

3.6. Extracting method

- Use the zigzag method to extract the cipher text from watermark.

Cipher text = 19,23,97,28,14,5,5,1,92

- Apply the SRSA to decrypt the output

Plain text =19,12,13,7,14,5,5,1,8

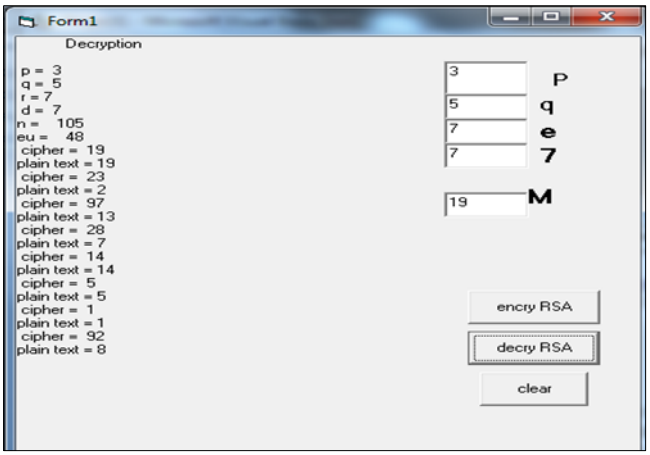

Figure 3 Implementation of SRSA

Apply Move–to – front coding algorithm as shown in table 2 below:

Table 2 Applying MTF method

Numbers	Extracted letter	English letters
19	S	Abcdefghijklmnopqrst
19,2	Sa	Sabcdefghijklmnopqrt
19,2,13	Sal	as bcdefghijklmnopqrst
19,12,13,7	Sale	las bcdefghijkmnopqrst
19,12,13,7,14	Salem	elas bcdfghijkmnopqrst
19,12,13,7,14,5	Salems	melas bcdfghijknopqrst
19,12,13,7,14,5,5	Salemsa	smela bcdfghijknopqrst
19,12,13,7,14,5,5,1	Salemsaa	asmel bcdfghijknopqrst
19,12,13,7,14,5,5,1,8	Salemsaad	dasmel bcfghijknopqrst

Message = Salemsaad

4. Conclusion

For the protection of buyers from cheating and preventing the fraud products to be expand in the market, a method of hiding the name of the original buyer as a watermark within the product. If any person tries to forge the product information or replicate it in an illegal form, then the fraud will be detected by examining the watermark on that product. The proposed method suggested a new approach of authenticating the buyer by watermarking his name within the product in the logo of the production company.

Compliance with ethical standards

Acknowledgments

The authors would like to thank the staff of Al_Ma'moon University college for their support.

Disclosure of conflict of interest

Both authors certify that they have participated sufficiently in the work to take public responsibility for the content.

References

[1] Cvejic, Nedeljko, Algorithms for audio watermarking and steganography Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu, P.O.Box 4500, FIN-90014 University of Oulu, Finland. 2004.

[2] S Voloshynovskiy, A Herrigel, N Baumgaertner, T Pun. A stochastic approach to content adaptive digital image watermarking, International workshop on information hiding. 211-236.

[3] Voloshynovskiy S, S Pereira, T Pun, JJ Eggers, JK Su. Attacks on digital watermarks Classification, estimation based attacks and benchmarks. IEEE. Commun. Mag. 2011; 39: 118-126.

[4] Karzenbeisser S, F Perircolas. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, ISBN: 1580530354. 2000; 240.

[5] Lee GJ, Yoon EJ, Yoo KY. A new LSB based Digital Watermarking Scheme with Random Mapping Function", in 2008 IEE.

[6] Titty T. Steganography: Reversible Data Hiding Methods for Digital Media. Bachelor project.

[7] CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE, FIFTH EDITION William Stallings Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall.

[8] COMPUTER SECURITY AND CRYPTOGRAPHY, ALAN G. KONHEIM, Copyright # 2007 by John Wiley & Sons, Inc. All rights reserved ,Published by John Wiley & Sons, Inc., Hoboken, New Jersey

[9] JL Bentley, CC McGeoch. Amortized analyses of self-organizing sequential search heuristics. Comm. ACM. 1985; 28: 404–411.

[10] S Ahmed, S Abdualazize. Embedding Secrete Message in Transformed Voices File using a New Method for Position Selection", Electronic ISBN: 978-1-5386-9188-5, Print on Demand (PoD) ISBN: 978-1-5386-9189-2. 14 February 2019.

[11] S Ahmed, S Abdualazize. Preventing Unauthorized Access to Special Applications using Signed Audio, International Journal of Civil Engineering and Technology (IJCIET), CiteScore:2.76, SJR:0.246, SNIP:0.153, Impact Factor:9.7820 , ISSN:0976-6316.

[12] S Ahmed, S Abdualazize. A Proposed Method for Image Verification by Encrypted Hidden Text using a Chaotic Polynomial and Random Locations, International Journal of Civil Engineering and Technology (IJCIET), CiteScore:2.76, SJR:0.246, SNIP:0.153, Impact Factor:9.7820 , ISSN:0976-6316.