International Journal of Information & Network Security (IJINS)
Vol.3, No.2, April 2014, pp. 83~91
ISSN: 2089-3299

A Novel Approach of Amazigh Text Steganography based Elliptic Curve

Hassain Sadki*, Fatima Amounas, El Hassan El Kinani*****
*R.O.I Group, Computer Science Department, Moulay Ismail University, Faculty of Sciences and Technics Errachidia
**R.O.I Group, Computer Science Department, Moulay Ismail University, Faculty of Sciences and Technics Errachidia
***A.A Group, Mathematical Department, Moulay Ismail University, Faculty of Sciences and Technics Errachidia,

Article Info

Article history:

Received Jan 12th, 2014
Revised Feb 20th, 2014
Accepted Mar 16th, 2014

Keyword:

Information Hiding
Cover Text
Mapping Technique
Stego Text
Text Steganography.

ABSTRACT

Techniques for information hiding are becoming increasingly more sophisticated and widespread. Steganography is the art and science of hiding information by embedding data into media. Over the years we have come across several steganographic techniques designed for hiding information inside digital media like image, audio and video files etc. Text steganographic is more difficult than others because there is a little redundant information in text file. In this paper, we attempt to provide a new steganographic method for hiding information inside Amazigh Unicode text documents. This approach combines schemes of cryptography with steganography for hiding secret messages. Therefore, the proposed method has a high hiding capacity because it inserts one character at each time instead of hiding one bit in the existing methods. Moreover, our algorithm can be applied in different size textual data.

Corresponding Author:

E.H. El KINANI
Mathematical Department Moulay Ismail University,
Faculty of Sciences and Technics, Box 509 Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

1. INTRODUCTION

Information hiding is the ability to prevent or hidden certain aspects from being accessible to others excluding authentic user. It has many sub disciplines. One of the most important sub disciplines is steganography [1, 2]. In fact, steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is in the appearance in the processed output. In steganography, the output is not apparently visible but in cryptography the output is scrambled so that it can draw attention.

Several of steganography works have been carried out on image, video clip and sound [3, 4, 5, 6]. In Image Steganography method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes. In video steganography, same method may be used to embed a message. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [7]. One major category, perhaps the most difcult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio. Different algorithms have been presented to hide data inside text files. Some of these methods were designed to be applied in specific languages [8, 9].

Languages and their structures play differences in the preferred steganographic system. Normally no single technique is to be used for all languages [10]. The Figure 1 shows the mechanism of text steganography. Firstly, a secret message will be covered up in a cover-text by applying an embedding

algorithm to produce a stego-text. The stego-text will then be transmitted by a communication channel to a receiver.

In our previous works, we have provided cryptographic algorithms based on ECC mechanism [11, 12, 13, 14]. The transformation of the message into affine points is explained in [15]. Moreover, we have introduced the elliptic curve cryptography using Amazigh alphabet in [16,17,18]. In this paper, an approach of text steganography method for Amazigh characters has been proposed. More precisely, we suggest an algorithm to hide the amazigh letter using a text file as a carrier. This work extends a point multiplication methodology from our previous work [19]. The remaining parts of this paper is developed as follows: Section 2 investigates the basic theory of elliptic curve and provides an overview of Amazigh alphabet. Section 3 describes the proposed model. Algorithms of various processes like embedding and extracting are discussed in this section. The last section describes the concluded part of the work.

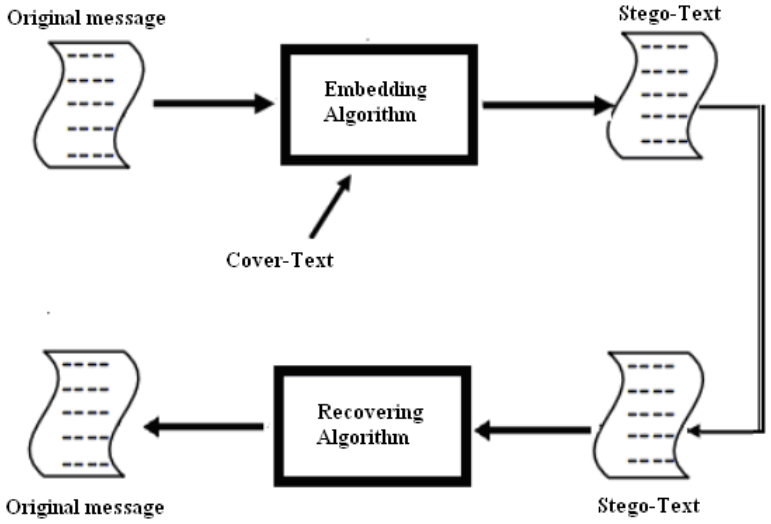

Figure 1. The mechanism of text Steganography

2. BRIEF REVIEW ON ELLIPTIC CURVE AND UNICODE

2.1. Elliptic Curve

According to [20], elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications [20].

An elliptic curve E over a field F_p denoted by E/F_p is given by the Weierstrass equation:

$$y^2 = x^3 + ax + b \bmod p; \quad (1)$$

where x, y are elements of field F_p and a, b are integer modulo p, satisfying the following equation:

$$4a^3 + 27b^2 \neq 0 \bmod p; \quad (2)$$

Here 'p' is known as modular prime integer making the EC finite field. An elliptic curve E over F_p consist of the solutions (x, y) defined by (1) and (2), along with an additional element noted Ω, which is the point of EC at infinity. The set of points (x, y) are said to be affine coordinate point representation. In our case, we are interested to extend the properties of elliptic curve in text steganography.

2.2. UNICODE

Unicode is a character encoding standard that has widespread acceptance. Unicode defines a large number of characters and assigns each of them a unique number, the Unicode code, by which it can be

referenced. This encoding standard provides the capacity to encode all of the characters used for the written languages of the world. The objective of Unicode is to unify all the different encoding schemes so that the confusion between computers can be limited as much as possible. The most common Unicode encodings are called UTF-n, where UTF stands for Unicode Transformation Format and n is a number specifying the number of bits in a basic unit used by the encoding. Two very common encodings are UTF-16 and UTF-8. In this paper, we are investigated encoding UTF-8 for Amazigh alphabet. In UTF-8, which is used in pratice, each Unicode character is represented as one or more bytes. The benefit of Unicode is that, it assigns each character a unique value and symbol, no matter what the platform, no matter what the program, no matter what the language.

2.3. Amazigh Alphabet

The Tifinagh alphabet adopted by the Moroccan Royal Institute of the Amazigh Culture (IRCAM) was officially recognized by the international organization of standardization (ISO). The Table 1 presents the associated Unicode allocated by ISO. Amazigh alphabet is encoded in the Unicode range U+2D30 to U+2D7F. There are 55 characters defined by ISO. According to researchers, the name Tifinagh is compound of two words: Tifi (that is discovering) and Nagh (that is ones self). IRCAM has proposed a standardization of Tifinagh characters composed of 33 elements. The form of Tifinagh which is recognized and used by IRCAM is shown in Figure 2.

A B g Å d Ä e f k Æ h p o X Q I J L M U R Ë v s Ã c T Ï w Y z Ç

Figure 2. Tifinagh characters adopted by IRCAM.

Table 1. Encoding of Characters Amazigh.

Code	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F
U+2D30	A	B	Ý	g	Á	Ø	â	d	Õ	Ä	À	e	f	k	Ö	ß
U+2D40	h	×	Ì	p	o	G	Í	q	Ô	i	j	ü	ú	l	m	n
U+2D50	È	É	Ñ	U	r	Ë	v	Î	ê	s	Ã	c	T	Ù	þ	ï
U+2D60	Ÿ	W	Y	z	Û	ç	>	--								µ
U+2D70																

3. MAIN CONTRIBUTION

In this section, a new steganography scheme is provided for hiding text in a cover-text. The embedding process will represent one character Amazigh by a group of codes point. Specially, we define the mapping F as specified rule of correspondence between sets of binary codes: 00, 01, 10 and 11, which are composed message and a set of codes representation. Each character had been converted into Unicode representation, depending on the assumption of 00, 01, 10 and 11. For enchancing the security of the message, the elliptic curve algorithm has been used in the proposed approach. Our idea is to hide data inside a text file without any change in the file format.

3.1. Proposed Approach

In this approach the two algorithmic process is described one for the Sender Side and another for the Receiver Side. The first one consists of two building blocks: Encryption Algorithm which enciphers a message using ECC method and Hide function which conceals the scrambled message using the mapping technique. The second consists of two building blocks: Seek function which extracts the hidding information from the stego file and Decryption algorithm which deciphers the extracted message using ECC.

In this method cover text and encrypted message is generated by the user. The system will search out the corresponding group of characters which are mapped with that the current character. Secret message has been embed to the cover text by inserting that particular group of letters based on the mapping information shown in Figure 3 to form the stego text. For to enhance the security, the message has been embed to the cover text by inserting the Unicode representation to form the stego text. At the receiver side other different reverse operation has been carried out to get back the original information.

Let us assume we have an elliptic curve E defined over finite field F_p. P is a point generator of order n.

A	00	01	10	11
	B	Ý	g	Á
	2D31	2D32	2D33	2D34

B	00	01	10	11
	Ý	g	Á	Ø
	2D32	2D33	2D34	2D35

...

Z	00	01	10	11
	Û	ç	>	--
	2D64	2D65	2D66	2D67

ç	00	01	10	11
	>	--	µ	A
	2D66	2D67	2D6F	2D30

Figure 3. Mapping technique.

a) Encryption Algorithm

Input: original message
Output: cipher text

- Take plaintext message, and encodes it onto a point P_i (i=1, 2,...) from the elliptic curve. All points are stored into matrix of (r × 2), noted M.
- Choose a non-singular matrix of (2 × 2) such that |A| = 1.
- Compute the product: C = MA. The cipher text is a set of points C_i; i =1, 2,...

b) Hide Function

Input: cover-text & cipher text
Output: stego-text to send

1. Encrypt the secret message in text form (input file). Then, select the cover text to embed the message. Check whether the selected text is capable of embedding. If not possible repeat this step otherwise continue.
2. Read a character from the file and convert it into corresponding binary code.
3. Pack out two pair of bit stream of result message (b_ib_j) one by one and change it to it's equivalent code representation using mapping technique. If b_ib_j='00' then find out the first character from the group selected. Similarly, '01', '10', '11'.
4. Circularly, read a bit (s) from least signifiant bit (LSB) to most signifiant bit (MSB) of the secure key (mP). If s = 1 then the Unicode representation of the character in the cover text could be inserted in the stego file. Else if s = 0, write the Unicode representation of the character in the encrypted message in the stego file.
5. Repeat steps 2 to 4 till the end of the file and the cover text. Then, write m in the stego key.
6. Return stego-text file.

The stego file and stego key are sent separately to the receiver.
At the receiver side with the help of same mapping algorithm and other different reverse operation has been carried out to get back the original information.

c) Seek Function

Input: stego-text & stego key.
Output: cipher text & cover-text

1. Read a value from the stego key and get the corresponding code of mP.
2. Read 'm' characters from the stego file. Circularly get a bit position from least signifiant bit (LSB) to most signifiant bit (MSB) of the binary sequence.
3. Depending on binary bit (s), the choice to select the cipher text or cover text is made. Select m/2 characters from the current stream with the bit position 1 and convert it to binary sequence using mapping technique and into corresponding letter. Similarly for the next block with bit position 0. If s=1 then write the letter in the cover text, else if s=0 then write the letter in the cipher text. Repeat the process for the remaining characters.
4. Repeat steps 2-3 until stego file is finished.
5. Return the extacted message.

d) Decryption Algorithm

Input: Cipher text & secure key
Output: Original message

1. Extract a points C_i from the cipher text . Then stored data points in matrix of ($r \times 2$).
2. The encoded message M is again decoded using the inverse of A, i.e perform the product $M = CA^{-1}$

3.2. Illustration and Results

In this section, we show the details of our algorithm by an example. The elliptic curve using here is given by the following equation:

$$y^2 = x^3 + 4x + 20 \bmod 29; \quad (3)$$

The base point P is selected as (1, 5). In our case we use the Tifinagh characters (Tifinagh IRCAM) with some of the other symbols like ';', '(', ')' and space for illustration purpose only. Here, Unicode code (code point) will be enough to represent the 33 characters of Tifinagh IRCAM. We use some other codes to hide symbols: ';', '(',')', space inside the message. These codes are illustrated in Table 2.
The meaning of code point is a particular integer that is being used to code the abstract character [21]. The standard understanding of code points in the Unicode Standard is to refer code point as their numeric value assigned in hexadecimal, with a "U+" prefix.
Here, we show an example to detail this steganography process. Assume that the binary code of secret key (0110110111), looking from the least significant bits to be started with. The first bit found is 1, then the current representation code of the character in the covertext could be inserted into stego file. The fourth bit found is 0, then the current representation code of the character in the cipher text could be inserted into stego file. We execute above operation repeatedly till the end of the data sequence. Then, convert the obtained codes into characters equivalent. The Figure 4 gives the corresponding bits position.
In our case, we choose matrix A as:

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

Consider a message "**S TIRA N TIFINAgh**" to be hidden. After enciphering the message, cipher text generated was "**ssÇBVsgËmæzgmBuhh**".

The secret message to be embedded, encrypted message and cover text are given as following:

Data to hide	Encrypted message	Cover text
S TIRA N TIFINAgh	**ssÇBVsgËmæzgmBuhh**	**TANMIRT I TAYMUnT N UZRY**

The above mentioned technique has been implemented using secret key. The data is embedded into the point on elliptic curve and encrypted using non-singular matrix. The Unicode representation could be inserted to represent the characters of the secret message between any two bits of the cover text according to embedding algorithm. The results are shown in the following figures (Figure 5, Figure 6, Figure 7).

```
11101101101110110110111011011011101101101110110110111011011011101101101110110
11011101101101110110110111011011011101101101110110110111011011011101101101110
11011011101101101110110110110110110
```

Figure 4. Bit position

Code representation of Cover text									
2D5E	2D60	2D5D	2D5E	2D5F	2D5D	2D5D	2D5F	2D5E	2D5E
2D53	2D51	2D53	2D52	2D53	2D4F	2D50	2D4F	2D50	2D51
2D4A	2D4A	2D4B	2D4B	2D4C	2D55	2D56	2D57	2D57	2D55
2D5E	2D60	2D5D	2D5E	2D5F	0020	0020	0020	0020	0028
2D4A	2D4A	2D4B	2D4B	2D4C	0020	0020	0020	0020	0028
2D5E	2D60	2D5D	2D5E	2D5F	2D5D	2D5D	2D5F	2D5E	2D5E
2D65	2D63	2D65	2D65	2D65	2D4F	2D50	2D4F	2D50	2D51
2D54	2D54	2D54	2D55	2D57	2D53	2D51	2D53	2D52	2D53
2D5E	2D60	2D5D	2D5E	2D5F	0020	0020	0020	0020	0028
2D53	2D51	2D53	2D52	2D53	0020	0020	0020	0020	0028
2D54	2D54	2D54	2D55	2D57	2D64	2D67	2D65	2D64	2D65
2D55	2D56	2D57	2D57	2D55	2D65	2D63	2D65	2D65	2D65

Figure 5 . Cover text

Code representation of cipher-text									
2D5C	2D5B	2D5D	2D5A	2D5A	2D5C	2D5B	2D5D	2D5A	2D5A
2D67	2D30	2D6F	2D66	2D6F	2D32	2D34	2D33	2D32	2D35
2D59	2D57	2D57	2D57	2D59	2D5C	2D5B	2D5D	2D5A	2D5A
2D36	2D36	2D34	2D34	2D37	2D56	2D58	2D58	2D57	2D59
2D4F	2D50	2D4F	2D50	2D51	2D63	2D64	2D65	2D63	2D65
2D64	2D67	2D65	2D64	2D65	2D36	2D36	2D34	2D34	2D37
2D4F	2D50	2D4F	2D50	2D51	2D32	2D34	2D33	2D32	2D35
2D54	2D54	2D54	2D55	2D57	2D63	2D64	2D65	2D63	2D65
2D42	2D42	2D42	2D44	2D42	2D42	2D42	2D42	2D44	2D42

Figure 6. Encrypted Message to be embedded

2D5E	2D60	2D5D	2D5C	2D5E	2D5F	2D5B	2D5D	2D5D	2D5D
2D5F	2D5E	2D5E	2D5A	2D53	2D51	2D5A	2D53	2D52	2D5C
2D53	2D4F	2D50	2D5B	2D4F	2D50	2D5D	2D51	2D4A	2D5A
2D4A	2D4B	2D4B	2D5A	2D4C	2D55	2D67	2D56	2D57	2D30
2D57	2D55	2D5E	2D6F	2D60	2D5D	2D66	2D5E	2D5F	2D6F
0020	0020	0020	2D32	0020	0028	2D34	2D4A	2D4A	2D33
2D4B	2D4B	2D4C	2D32	0020	0020	2D35	0020	0020	2D59
0028	2D5E	2D60	2D57	2D5D	2D5E	2D57	2D5F	2D5D	2D57
2D5D	2D5F	2D5E	2D5C	2D5E	2D65	2D5B	2D63	2D65	2D5D
2D65	2D65	2D4F	2D5A	2D50	2D4F	2D59	2D50	2D51	2D5A
2D54	2D54	2D54	2D36	2D55	2D57	2D36	2D53	2D51	2D34
2D53	2D52	2D53	2D34	2D5E	2D60	2D37	2D5D	2D5E	2D56
2D5F	0020	0020	2D58	0020	0020	2D58	0028	2D53	2D57
2D51	2D53	2D52	2D59	2D53	0020	2D4F	0020	0020	2D50
0020	0028	2D54	2D4F	2D54	2D54	2D50	2D55	2D57	2D51
2D64	2D67	2D65	2D63	2D64	2D65	2D64	2D55	2D56	2D65
2D57	2D57	2D55	2D63	2D65	2D63	2D65	2D65	2D65	2D64
2D65	2D67	2D65	2D64	2D65	2D36	2D36	2D34	2D34	2D37
2D4F	2D50	2D4F	2D50	2D51	2D32	2D34	2D33	2D32	2D35
2D54	2D54	2D54	2D55	2D57	2D63	2D64	2D65	2D63	2D65
2D42	2D42	2D42	2D44	2D42	2D42	2D42	2D42	2D44	2D42

Figure 7. Stegano-Text generated

There are three parameters that should be taken into account when discussing the results of text steganography methods: security, capacity and robustness. In this work an attempt has been made to increase the level of security of the steganography model by incorporating the idea of secret key along with the use of encoded form of the original message. The above results showed that the approach used was found to satisfy both security aspects, hiding capacity requirements and minimal embedding time. It generates the stego text without change text form which is not very revealing to people about the existence of any hidden data, maintaining its security to the eavesdroppers.

The levels of security incorporated in the proposed model: i) Generation of the encrypted form of the secret message. ii) Use of the secret key and embedding encrypted form of the message in cover text to form the stego text using the proposed method. Besides the security level has amplified through the encoding of the secret message before embedding operation. This method hides one character in the cover text which reflects the high embedding capacity of the system.

Our model has some main advantages which are listed below:

- File format will not be affected by embedding the stego data.
- This algorithm improves the transparency feature since the stego file format seems as the original file.
- Hiding capacity: The users can determine where the suitable place to insert Unicode characters would be.

Moreover, Tifinagh is the official language in Morocco and it can be used on different systems and devices through the world. As a result, a wide range of the users can use our method.

4. CONCLUSION

In this paper, a new mechanism for hiding information in Amazigh text using elliptic curve has been presented. In this approach different codes are used as tools to represent Unicode character with the help of the mapping technique. This method is not dependant on any special format and we can save the stego text in different formats such as HTML, Microsoft word, etc, because the stego Unicode text will not change during this process. The proposed steganography technique is a new approach for the Amazigh steganography and this methodology can be extended to other language. Finally, the result shows that the performance of the technique is satisfactorily. The future work should be focused to improve the capacity of the embedding scheme by incorporating some complex technique on the secret message as well as using the genetic function and the compression technique.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referee for their valuable comments and suggestions.

REFERENCES

[1] Ross J. Anderson Fabien A.P. Petitcolas and Markus G. Kuhn ,"Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062-1078, 1999.
[2] Kessler c. Gary, "An Overview of Steganography for the computer Forensics Examiner, " *Forensics Science Communications*, vol 6, no. 3, 2004.
[3] N. Provos and P.Honeyman, "Hide and seek an introduction to steganography, " IEEE security and Privacy, vol. 3, pp. 32-44, 2003.
[4] R.chandramouli and N.Menon, "Analysis of LSB based image steganographic technologies, " *Proceedings of the International conference on Image Processing*, vol. 3, pp. 1019-1022, 2001.
[5] G.Doerr and J.L.Duglay, "A guide tour of video watermarking, " *Signal Processing: Image communication*, vol. 18, no. 4, pp. 263-282, 2003.
[6] G. Davida M. Chapman and M. Rennhard., "A practical and effective approach to large-scale automated linguistic steganography," *In Proceedings of the Information Security Conference*, pp. 156-165, 2001.
[7] K.Gopalan, "Audio steganography using bit modifications, " *Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'03)*, vol. 2, pp. 421-424, 2003.
[8] R. Prasad, K. Alla, "A New Approach to Telugu Text Steganography," *Proceedings of the IEEE Wireless Technology and Applications Conference (ISWTA)*, pp. 60-65, 2011.
[9] L. Yuling, S. Xingming, G. Can, W. Hong, "An Efficient Linguistic Steganography for Chinese Text," *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 2094-2097, 2007.
[10] A. Rachidi and D. Mammass, "Informatisation de la langue amazighe: Méthodes et mises en oeuvre, " *SETIT 2005 3rd International Conference: Sciences of Electronic Technologies of Information and Telecommunications*, pp. 27-31, 2005.
[11] F.Amounas and E.H. El Kinani, " Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography, "*International Journal of Information & Network Security*, vol. 1, no. 2, pp. 54-59, 2012.
[12] F.Amounas and E.H. El Kinani, "Elliptic curve digital signature algorithm using boolean permutation based ECC, "*International Journal of Information & Network Security*, vol. 1, no. 3, pp. 216-222, 2012.
[13] F.Amounas, E.H. El Kinani and H.sadki, " An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem,"*International Journal of Information & Network Security*, vol. 2, no. 3, pp. 253-259, 2013.
[14] F.Amounas, E.H. El Kinani and M.Hajar, " Novel Approach for Enciphering Data based ECC using Catalan Numbers, "*International Journal of Information & Network Security*, vol. 2, no. 4, pp. 339-347, 2013.
[15] F.Amounas, E.H. El Kinani, and A. Chillali, "An application of discrete algorithms in asymmetric cryptography, " *International Mathematical Forum*, vol. 6, no. 49, pp. 2409-2418, 2011.
[16] F.Amounas and E.H. El Kinani, "Cryptography with elliptic curve using tifinagh characters, "*Journal of Mathematics and System Science 2*, pp. 139-144, 2012.
[17] F.Amounas and E.H. El Kinani, "Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet, "*International Journal of Information & Network Security*, vol. 2, no. 1, pp. 43-53, 2013.
[18] F.Amounas and E.H. El Kinani, "A novel encryption scheme of Amazigh alphabet based elliptic curve using pauli spin 1/2 matrices, "*International Journal of Information & Network Security*, vol. 2, no. 2, pp. 190-196, 2013.
[19] F.Amounas and E.H. El Kinani, "An efficient elliptic curve cryptography protocol based on matrices, "*International Journal of Engineering Inventions*, vol. 1, no. 9, pp. 49-54, 2012.
[20] Muhammad YasirMalik, "Efficient implementation of elliptic curve cryptography using low-power digital signal processor, " ISBN 978-89-5519-146-2 ICACT, 2010.
[21] Web reference: http://www.unicode.org [As accessed on: 02-November- 2012]

Appendix

Table 2. Codes representation for Tifinagh Characters.

Ch.	Point	Code representation	Ch.	Point	Code representation
A	(1, 5)	2D5D2D5D2D5F2D5E2D5E	N	(27, 27)	2D532D512D532D522D53
B	(4, 19)	2D322D342D332D322D35	U	(0, 7)	2D542D542D542D552D57
G	(20, 3)	2D362D362D342D342D37	R	(3, 8)	2D552D562D572D572D55
Å	(15, 27)	2D472D492D492D482D49	Ë	(5, 7)	2D562D582D582D572D59
D	(6, 12)	2D382D3B2D382D3B2D38	V	(16, 2)	2D592D572D572D572D59
Ä	(17, 19)	2D3C2D3A2D3D2D3C2D3D	S	(19, 16)	2D5C2D5B2D5D2D5A2D5A
e	(24, 22)	2D3F2D3C2D3D2D3D2D3C	Ã	(10, 4)	2D5D2D5D2D5C2D5D2D5C
F	(8, 10)	2D3E2D3D2D3D2D3F2D3F	C	(13, 6)	2D602D612D612D602D61
K	(14, 23)	2D3F2D412D3F2D3F2D41	T	(14, 6)	2D5E2D602D5D2D5E2D5F
Æ	(13, 23)	2D632D642D652D632D65	Ï	(8, 19)	2D612D602D612D602D63
H	(10, 25)	2D422D422D422D442D42	W	(24, 7)	2D652D622D622D632D65
P	(19, 13)	2D462D452D462D472D45	Y	(17, 10)	2D652D632D652D652D65
O	(16, 27)	2D472D452D462D472D48	Z	(6, 17)	2D642D672D652D642D65
X	(5, 22)	2D5E2D602D612D5F2D60	Ç	(15, 2)	2D672D302D6F2D662D6F
Q	(3, 1)	2D482D492D4A2D482D49	;	(20, 26)	00290029002800290029
I	(0, 22)	2D4A2D4A2D4B2D4B2D4C	(	(4, 10)	00200029002000290029
J	(27, 2)	2D4E2D4C2D4D2D4B2D4D	)	(1, 24)	00200020003B00290020
L	(2, 23)	2D4E2D4F2D4F2D502D51	Space	Ω	00200020002000200028
M	(2, 6)	2D4F2D502D4F2D502D51			

BIOGRAPHY OF AUTHORS

HASSAIN SADKI received the Ph.D degree in Physics, Computer Science and their applications in 2000 from Moulay Ismail University, Morocco. He is currently an Assistant Professor at Computer Science department at the Faculty of Sciences and Technics, Errachidia, Morocco. His research interests include information security.

FATIMA AMOUNAS received the Ph.D degree in Mathematics, Computer Science and their applications in 2013 from Moulay Ismail University, Morocco. She is currently an Assistant Professor at Computer Science department at the Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

EL HASSAN EL KINANI received the Ph.D in Mathematical Physics in 1999 from Mohamed V University Rabat Morocco. He is full Professor at department of mathematics in Moulay Ismail University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested including classical and quantum cryptography.