Authentication using Hidden Encrypted Barcode

Sana Ahmed Kadhom
Al Maamon College University, Computer Science Department
Sana_ahmed73@yahoo.com

Received 23 October 2013 ; Accepted 9 January 2014

Abstract

Barcode is used to determine not only the price of the product but also to protect companies' rights by preventing copycat. Encryption, in the other hand, is used to make the information unreadable and not forgeable. It is used in trading and political mails also it is used in banks for money transfer.

The authentication in this research was built for persons who work in security companies and governmental institutes, but for simplicity access to students' identification cards they were used in implementations.

In this research student's information were encrypted then converted into barcode, this barcode was added to student's identification card as a hidden watermark. The barcode will be used for verifying authenticity.

Keywords: barcode, cryptography, authentication, hiding.

التحقق من الموثوقية باستخدام الباركود المشفر المخفي

سناء احمد كاظم
كلية المأمون الجامعة, قسم علوم الحاسوب
Sana_ahmed73@yahoo.com

الخلاصة

لم يعد استخدام الباركود محدودا في معرفة اسعار البضائع ولكن ايضا لحفظ حقوق الملكية للشركات. من جهة اخرى يستخدم التشفير لجعل البيانات غير مقروءة ولا يمكن تزويرها وتستخدم هذه التقنية في المراسلات التجارية والسياسية وكذلك في التبادلات المالية في البنوك.

الطريقة المقترحة للموثوقية في هذا البحث بنيت في الاساس للاشخاص العاملين في المؤسسات الامنية والدوائر الحكومية الخاصة وتم استخدام هوية الطالب في تطبيقات البحث لسهولة الوصول والتعامل مع هذه الهويات.

في هذا البحث تم تشفير المعلومات الشخصية للطالب ثم تحويلها الى باركود, يتم اخفاء هذا الباركود في هوية الطالب ومن ثم يستخدم لاغراض التحقق من موثوقية الهوية.

الكلمات الدالة: الباركود, التشفير, التحقق من الموثوقية, الاخفاء.

Introduction

A standard bar code is a series of varying width vertical lines (called bars) and spaces. Bars and spaces together are named "elements". There are different combinations of the bars and spaces which represent different numbers. The type of barcode to use for a particular situation depends upon: (1) the implementation; (2) the data-to-encode in the barcode and (3) how the barcode will be printed. There are several different types of barcode standards for different purposes - these are called symbologies. Each type of symbology (or barcode type) is a standard that defines the printed symbol and how a device such as a barcode scanner reads and decodes the printed symbol[1].

Encryption is the process of converting the readable text to unreadable one. By using the substitution cipher we replace each character in the original text with another character or symbol.

Steganograhy is the art and science of hiding information by embedding messages within other, seemingly harmless messages. This hidden information can be plain text, cipher text, or even images. Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide

information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen[2]

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be[3]

By combining all the above aspects we can have a secured authentication system that can be used in universities, ministries, companies and other institutions.

In this research an encryption method is used with some modification to be suitable to be used with barcodes. Building an alphabetic matrix using keyword is a known method only this time the keyword is created from the student's name after it encrypted using vigenere cipher with the student's ID number as an encryption key. The encrypted name is converted to barcode and hidden in the student's identification card as a watermark.

Least significant bit (LSB) hiding

LSB based technique is most simple and straightforward approach in which message bits are embed in least significant bits of cover image. In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the secret message [4].

In the case of 24 bit color image each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. **[R (8 bits), G (8 bits) , B (8 bits)]**.

Suppose RGB of the first pixel can be represent as

[11011100 11000110 10000111]

For embedding secret image whose first pixel is [11001001] firstly we have to replace last 2 LSB of each of RGB component and then embedding first 2 most significant bits (MSB) of first pixel of secret image to R component, then next 2 MSB of first pixel of secret image to G component and lastly another next 2 MSB of first pixel of secret image to B component. In this way we get stego image whose first pixel is:

[11011111 11000100 10000010].

In this method 6 bits of secret image get hide by replacing only 2 bits of RGB component so stego-image is visually indistinguishable from the original cover-image in the case of 24 bit[5].

The Proposed Algorithm

Encryption part:

a- Take the student's first and last name; also take the ID number of the student to be used as an encryption key for vigenere cipher.

b- Encrypt the student's name; the result will be a cipher word with the same number of letters as the student's name.

c- The keyword will be used to build a (5 * 5) matrix; the keyword is the cipher word with no repetitions in the letters.

NOTE: wherever you find the letter "I" in the matrix put the letter "J" in the same position, and vice versa.

d- Columns are numbered starting from 0, rows are numbered starting from 5, so that we will get numbers between 0 and 9.

e- For each letter in the student's first name, find the row and the column number of that letter in the previous matrix. Two numbers will be obtained for each letter.

f- The final result will be a series of numbers (if the first name has "n" letters, then the series length will be n*2).

g- In the university database save the series numbers, the ID number and the name of the student as it is written in the identification card.

Barcode creation part:

a- Convert each number of the series you got to its equivalent barcode depending on the following standard barcodes.

b- Put the final result together.

c- Hide that barcode in the student's identification card.

Hiding the barcode part:

By using a hiding algorithm (LSB substitution algorithm) , hide the barcode image in the student's identification card. The barcode will not be visible anymore, it will be a watermark.

Authentication part:

To authenticate a student, many steps should be applied as follows:

a- Extract the barcode from the identification card.

b- Convert the barcode to its equivalent series of numbers using a barcode reader.

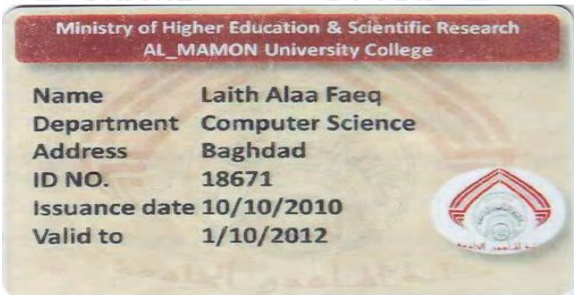
c- Search the university database for matching with that series.

d- If found match the data stored with that series (ID number and student's name) with the ID and the student's number from the identification card. If matched then the student is authenticated, otherwise the identification card is fake.

Implementation

Encryption and Creating barcode:

1. For the following student's identification card:



2. Take the student name (Laith Alaa) and encrypt it using viginer cipher and a key = 18671 (which is the ID NO.) to build the matrix.

Student name= LAITH ALAA

ID = 18671

Encryption process:

Key =	1	8	6	7	1	1	8	6	7
Name =	L	A	I	T	H	A	L	A	A
Cipher =	M	I	O	A	I	B	T	G	H

The keyword that will be used to build a (5 * 5) matrix will be :

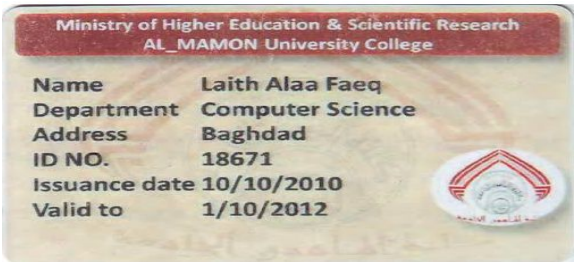
Keyword = MIOBTGH (cipher word with no repetitions)

Matrix = (NOTE: wherever you find I put J and vice versa).

	0	1	2	3	4
5	M	I/J	O	B	T
6	G	H	A	C	D
7	E	F	K	L	N
8	P	Q	R	S	U
9	V	W	X	Y	Z

3. For each letter in the student name (Laith), get the equivalent numbers:
   L=73 , a=62 , i=51 , t=54 , h=61
   Series = 7362515461
4. In the university database, save the following information:
   (ID no.= “18671” , Student’s name = “Laith Alaa Faeq” , Series numbers = “7362515461”)
5. Convert the series to the equivalent barcode:

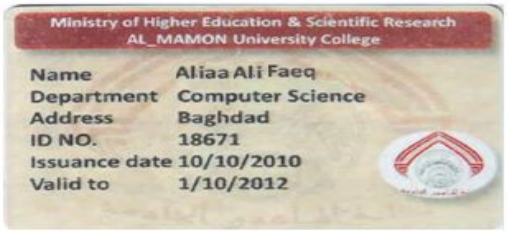
6. Hide the barcode in the student’s identification card:

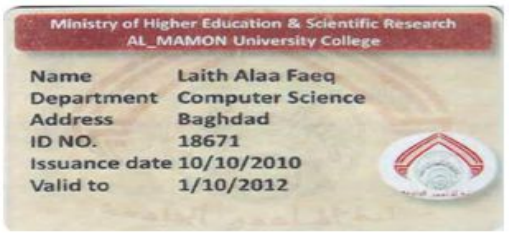


7. The barcode is hidden (invisible).

Authentication:

Assume the following two cards have to be authenticated.





1- Extract the barcode from the identification cards.

2- Convert the barcode to its equivalent series numbers.

Series = 7362515461

3- Search the university database for a matching with that series.

4- If found (extracted series = saved series) then match the ID no. and student's name from the cards with those in the database.

5- From the matching it appears that the first card is faked while the second one is original.

Evaluating the algorithm:

To evaluate the algorithm, suppose more than one student has the same name (Mohamed saad) but of course the ID number for each one is different. Suppose their ID's are of the same combinations as follows:

Ex: Student name 1= Mohamed Saad

ID 1= 18671

Encryption process:

Key =	1	8	6	7	1	1	8	6	7	1	1
Name =	M	O	H	A	M	E	D	S	A	A	D
Cipher =	N	W	N	H	N	F	L	Y	H	B	E

Keyword = NWHFLYBE

The matrix will be:

	0	1	2	3	4
5	N	W	H	F	L
6	Y	B	E	A	C
7	D	G	I/J	K	M
8	O	P	Q	R	S
9	T	U	V	X	Z

For Mohamed we get: M=74 , O=80 , H=52 , A=63 , M=74 , E=62 , D=70

The series will be = 74805263746270

74805263746270 =

For the second student:

Student name 2 = Mohamed Saad

ID 2 = 16871

Encryption process:

Key =	1	6	8	7	1	1	6	8	7	1	1
Name =	M	O	H	A	M	E	D	S	A	A	D
Cipher =	N	U	P	H	N	F	J	A	H	B	E

Keyword = NUPHFJABE

The matrix will be:

	0	1	2	3	4
5	N	U	P	H	F
6	I/J	A	B	E	C
7	D	G	K	L	M
8	O	Q	R	S	T
9	V	W	X	Y	Z

And the series will be:

Series2 = 74805361746370

For the third student:

Student name 3= Mohamed Saad

ID 3 = 1761

Encryption process:

Key =	1	7	6	1	1	7	6	1	1	7	6
Name =	M	O	H	A	M	E	D	S	A	A	D
Cipher =	N	V	N	B	N	L	J	T	B	H	J

Keyword = NVBLJTH

Then the series will be:

Series3 = 74806162747064

As it is clear from the previous example no confliction will be found in this algorithm since each student has its own ID number which is used in creating the keyword and then the matrix. Since the matrices are different then so as the barcodes even if the names of the students are the same.

Conclusions

1- The application field used in this research is a university and students. The proposed method was built to be used in other institutions such as governmental, security and private institutions.

2- The encryption matrix depends on part of the information within the student's identification card and each matrix is built after an encryption algorithm applied on the student's name, so each matrix will differ than other matrices for other students even if more than one student has the same name which is possible but then the ID number must differ and the barcode for the student name will be different, so in all cases, no two barcodes will be the same.

3- The barcode is easy in creating and reading by using the barcode reader, which is accessible to any user, so the proposed method is easy to implement and use.

4- For more security and to ensure authenticity, the barcode is watermarked in the student's ID card, so that it will not be seen or noticed to others.

5- More information could be added to the barcode like the student's birth date to increase secrecy and authenticity

References

1. http://www.barcodefaq.com/best-to-use.html , downloaded at 7/10/2013
2. http://www.webopedia.com/TERM/S/steganography.html , downloaded at 3/10/2013
3. http://searchsecurity.techtarget.com/definition/authentication , downloaded at 9/10/2013
4. Chan, C.K., Cheng, L.M., 2004. "Hiding data in images by simple LSB substitution". Pattern Recognition 37 (March), 469–474.
5. Deepesh Rawat , Vijaya Bhandari, 2013, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image ". International Journal of Computer Applications (0975 – 8887), Volume 64– No.20.