IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4522

MD5 Hash Function in Image Based Smart Card Security

Syed M Rahman
Department of Computer and Information Sciences, Minnesota State University, Mankato, MN 56001, USA, syedm@mail.mankato.msus.edu

Vincent Goh Boon Yew
Gippsland School of Computing and Information Technology, Monash University, Churchill, VIC, Australia 3842

ABSTRACT

The security of smart cards has raised a number of significant concerns over the years as they have become widely used. The potential for counterfeiting and fraud may pose significant financial risks to institutions issuing payment obligations in these systems and to other participants in these areas. Facial images or fingerprints for user authentication enhances smart card security to protect from illegal users. Attempt to alteration of image features need also to be protected.

Cryptography is one critical approach used to authenticate devices, information and messages. It protects data including images from unauthorized alteration or observations. However, smart cards have limitations on the memory space and computational power, and using image features would require comparatively larger space and computation time if encryption is to be used. There are proposals to use hash functions with cryptography as a solution, which may be computationally efficient. In this paper we studied the variations in an MD5 message digest for minor variations in image contents. The results show that even a slight change in an image content significantly changes the message digest. Changes in the set of shifting parameters in the algorithm also showed similar performance. We use this result to conclude that the MD5 hash algorithm with cryptography should protect the image content for user authentication.

1 INTRODUCTION

Smart card applications are spanning over various sectors of our life. Cashless payment, health care, social security, access control, authentication and retail loyalty bonus, are just a few examples of the applications. The move from individual cards for each application to a single card holding multiple applications for different purposes has only just begun. Due to co-residency of multiple applications, frequent data transfer, data privacy and the possibility of card loss, a need for multifaceted security measures is necessary.

Security Concerns: There are several significant security concerns including that if the physical security offered by smart card technology is adequate for the purposes for which they might be used. If security is compromised by inadequate systems, the resulting publicity could affect public confidence and reduce the scope for using cards – and indeed any computer storage of data in these areas [Hendry 1997].

The use of a card for electronic cash lead to it being used in a wide number of terminals in and outside the geographical boundary of a country. Many of which may be outside the direct and full control of the providing institution and may not be trusted. The institution will need to be confident that it's smart cards, when used in untrusted terminals, will be able to provide the needed level of protection for any private data held elsewhere on the card. Identification of the following participating component in the system are necessary.

i. Identification of user through the use of a PIN or biometrics. Use of biometrics appear more convenient and secure in identification of the user.
ii. Authentication of card: The card should have a mechanism for access to system to confirm that it is not counterfeit.
iii. Authentication of terminal: This card assures itself that the terminal, which is allowed to read or update information is genuine.

The vision of a multi-functional card that combines several applications on the same card is the future of smart cards. The smart card of the future will provide all the services previously mentioned, with the additional capability to keep various applications separated. In order to achieve this, each business system will have their own logic and data on the card, which will be private and protected. However, all applications will have access to shared data and services on the card, such as identification and security information. This will make the security issues more complicated. Use of smart card by illegal users and illegal terminals capturing information from a valid card are among the major security threats. Inclusion of protected facial images of the user and using the image information to authenticate between the card and the terminal may be a step to increased security [Rahman et al, 99]. MD5 hash algorithm is a well known hash algorithm that may be used to sign the content of an image. To protect the signature, a cryptographic algorithm on MD5 message digest may be used. In this paper, we provide experimental results to show that a MD5 hash algorithm produced message digest significantly changes for even minor changes in images and establish the suitability of the algorithm for this type of applications.

2 BIOMETRICS

A biometric identification procedure is one, which can identify a person unambiguously by unique, individual and biological properties. It may also distinguish between physiological and behavioural characteristics. A physiological characteristic is a relatively stable physical characteristic such as a fingerprint, retinal scan, hand geometry or facial features [McCrindle 1990]. An example of how smart card is used in conjunction with biometric features is detailed in the paper by Rahman et. al, 1999.

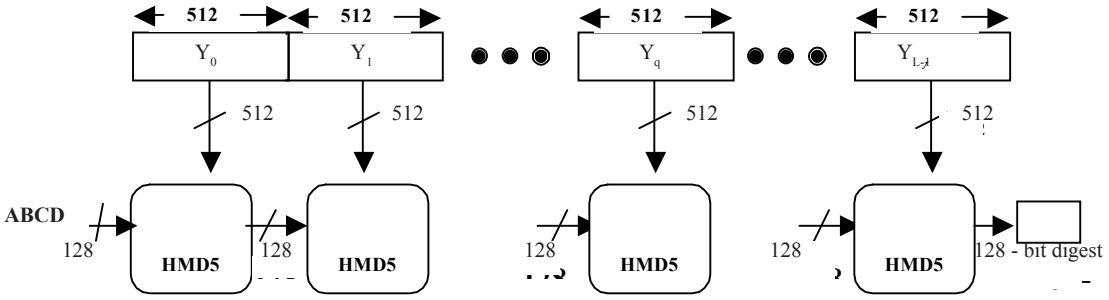
3 MD5 (MESSAGE DIGEST 5)

MD5 is a well-known hash function. MD4 and SHA are among others. A hash function H is a transformation that takes a variable-size input m and returns a fixed-sized string, which is called a hash value h given by: h = H(m). The hash value, h, may be appended to the message at the source at a time when the message is assumed or known to be correct. The receiver authenticates that message by recomputing the hash value. As the hash function itself is not considered to be secret, some means are required to protect the hash value.

MD4 is a precursor to MD5 developed by the same designer, Ron Rivest. Originally published as an RFC in October 1990, a slightly revised version was published as RFC 1320 in April 1992, the same date as MD5. MD5 share the same design goal as MD4, documented in a paper by Rivest. The main goals were to achieve in security, speed, simplicity and compactness, favour little-endian architecture (i.e. store the least significant byte of a word in the low-address byte position). MD5 was as an improved version of MD4. Although more complex than MD4, it is similar in design and also produces a 128-bit hash. The major differences included: four rounds of 16 steps in MD5 compared to three steps in MD4; use of additive constant in MD5; use of four primitive logic functions (one for each round) in MD5 compared to three in MD4; promoting a greater avalanche effect in MD5 by adding in each step the result of preceding steps.

Figure 1 depicts the simplified overall processing of a message to produce a digest. The processing consists of the following steps: appending padding bits, appending length, initialization of four 32-bit message digest buffers (A = 01234567, B = 89ABCDEF, C = FEDCBA98, D = 76543210), processing of message in 512-bit (16-Word) blocks and finally generation of a 128-bit message output digest. For further details see Stallings, 1995.

Figure 1. Message Digest Generation Using MD5 [Stallings 1995]



4 PERFORMANCE ANALYSIS

After investigating different security measures, MD5 is selected for this study due to the limitation of the smart card in terms of computational time and space. MD5 has been considered as a better choice due to the message digest generated being 128-bits and also due to the generation of the message digest being considerably faster than any other cryptography method.

The following are the objectives of this study:

- To study the variation of the signature digest generated by MD5 when images with slight changes are provided as input. The purpose of this study is to determine whether a change to any bit or bits in the image will result in a change to the message digest being produced.
- To study how the change in the shifting parameters affects the MD5 message digest. The purpose of this study is to determine whether changing the shifting parameters will create a substantial difference in the message digest being produced by MD5.

4.1 Effect of variation on same image

Experiment is conducted to study the effect of minimal variations on a type of image. Several pictures were taken for one person only by slightly changing his facial expression and all other parameters including position, orientation and light intensity etc. remaining the same. The following steps have been carried out for this experiment:

- MD5 is run on each image content to obtain a 128-bit message digest for each image.
- The information differences between message digest i and message digest j (id_{ij}) is calculated using the following formula.

$$id_{ij} = md_i \geq md_j$$

where, md_i md_j represents the MD5 message digest for the image numbers i and j respectively

- The distance ($dist_{ij}$) between message digest i and message digest j is calculated using the following formula.

$$dist_{ij} = \sum_{i=0}^{127} b_i$$

where, b_i is the value of bit at position i in id_{ij}.

- The histogram for the calculated distances $dist_{ij}$-s is constructed.

Experimental Setup: The experiment was performed on 60 images containing 50 images from the same person, varying some features in the facial regions, in different combination. It included 10 images with changes in facial expression only, 10 images with changes in intensity only, 10 images with changes in face and gestures movements only and 20 images with a combination of the above.

A second set of experiments was performed with 10 fingerprint images, and varying some features of the facial images as discussed below.

As for the 10 fingerprints, three of the fingerprints are from the same person and from the same finger but the difference between them is the amount of smearing with ink, either darker or lighter. The remaining fingerprints are from different person but from the same finger.

Results: Figure 2 shows the result of the experiment.

From the result it is evident that the total number of bits change ranges between 51 to 78 bits range out of 128 bits. It shows that, with a slight change in facial expression, intensity, movement in the facial image and change of these features in the fingerprint, the message digest produced a significant difference. These fulfil our purpose of using MD5.

Figure 2 Histogram for facial expression with slight changes

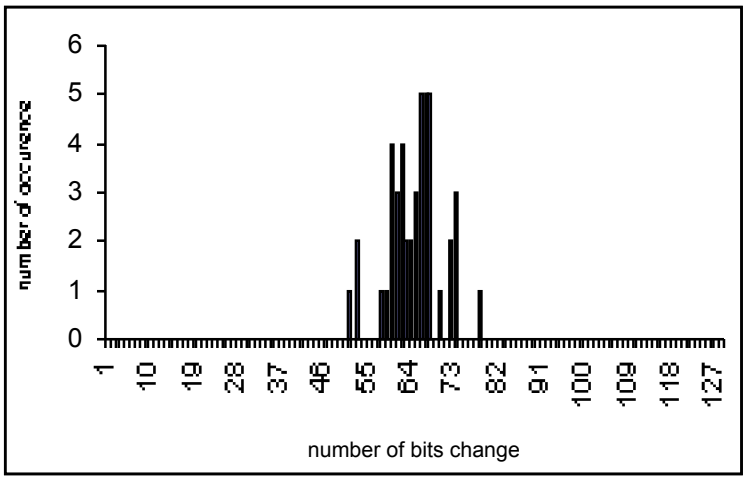


Table 1. Different shifting parameter values

	S11	S12	S13	S14	S21	S22	S23	S24	S31	S32	S33	S34	S41	S42	S43	S44
Original	7	12	17	22	5	9	14	20	4	11	16	23	6	10	15	21
Set1	6	11	16	21	4	8	13	19	3	10	15	22	5	9	14	20
Set2	31	1	7	8	9	15	13	29	20	23	5	7	13	16	21	19
Set3	20	25	30	35	13	17	22	28	11	18	23	30	2	14	19	25

4.2 Effect of shifting parameters

Experiments were carried out to test the effect of change in shifting parameters in the generation of the MD5 message digest on the same set of images and fingerprints using the same. The test set of the shifted parameter is shown in Table 1.

Results: Figure 3 shows four different histograms for four different set of shifting parameters. From the graph it is seen that the number of bits change are from 49 to 85. It shows that by changing the shifting parameters, the number of bits change are significant. This property of the MD5 may be used to change the shifting parameters to change the user identification parameter from application to application.

5 CONCLUSIONS

In conclusion, with hash functions such as MD5 an image can be hashed into a 128-bit message digest, by using either symmetrical or asymmetrical encryption techniques to encrypt the digest. This has advantages over encrypting the image itself. This will minimize the computational time and the response time by decreasing the data communication time over to the other side. MD5 appears considerably reliable as minor changes in the content produces significant changes in the message digest being produced, as discussed in the performance analysis chapter. The security level can be enhanced using different set of shifting parameter as a function of the user and time.

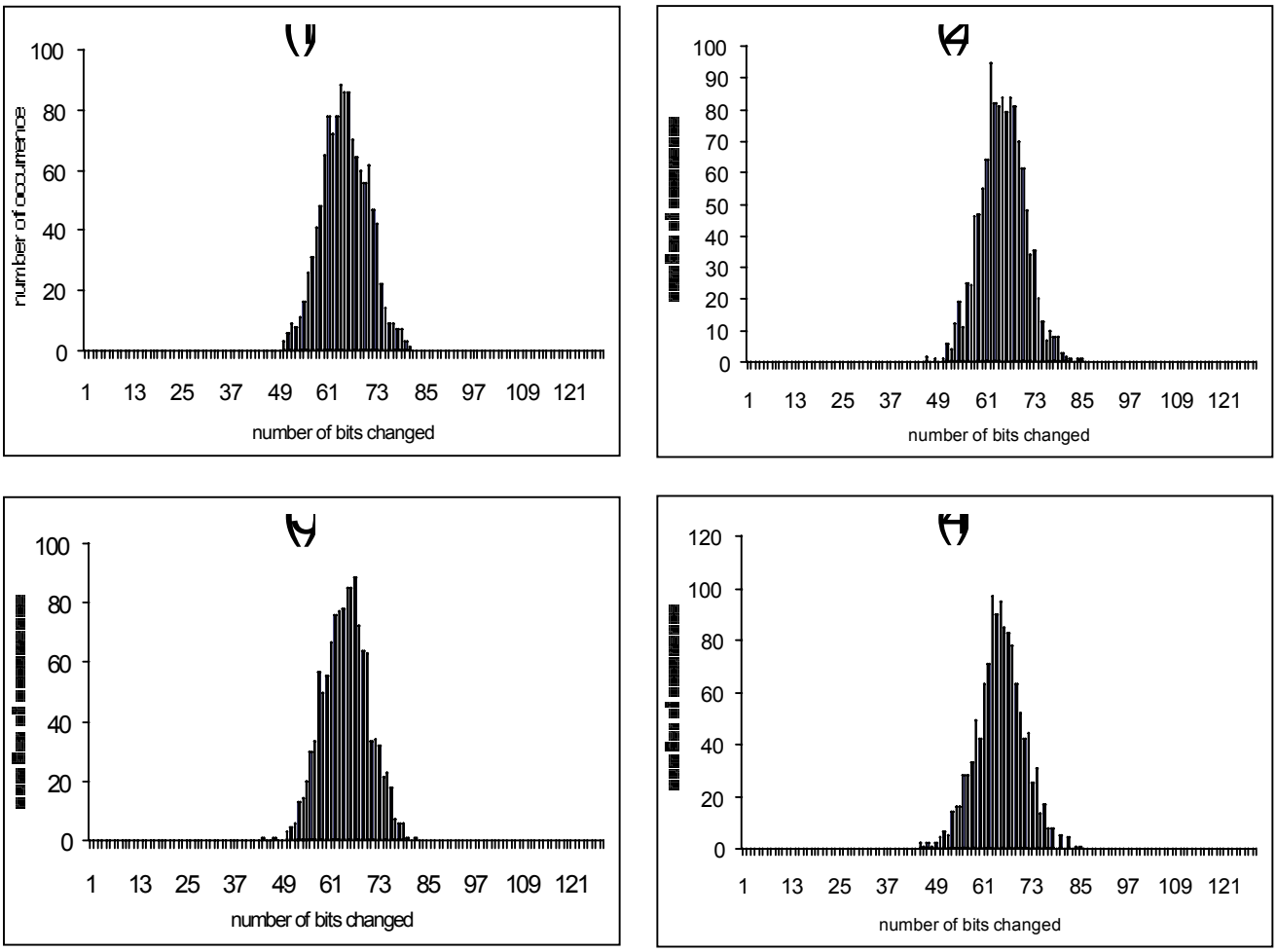


Figure 3 Four histogram for four different shifting parameters

REFERENCES

Hendry, Mike, "Smart Card Security and Applications", Artech House, Inc., 1997

Kaplan, Jack M, "Smart Cards : The global information passport : Managing a successful smart card program", London : International Thomson Computer Press, 1996

Konigs H.P. (1991): "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communications Magazine

McCrindle, J.A, "Smart Cards", Kempston, [England] : IFS Ltd UK, c1990

Rankl, W, "Smart Card Handbook", Chichester, New York : Wiley, c1997

Stallings, William, "Network and Internetwork Security : Principles and Practice", Prentice-Hall, 1995

Rahman S M, Rauniar D and Bignall R J: Biometric Authentication for Secure Smart Card Applications. Advances in Intelligent Computing and Multimedia Systems, Baden-Baden, Germany, 2-7 August 1999, pp.159-164.

Tomkowiak S, Hofland P.: "A computer in your wallet", BYTE magazine, 1996.

http://www.oberthurkirk.com/, "Smart Card Home Page" [Kirk, 1998].