Applications of Public Key Watermarking for Authentication of Job-Card in MGNREGA

Sirsendu Sarbavidya[1] and **Sunil Karforma**[2]

Submitted in July 2011; Accepted in December 2011

Abstract- ***Nowadays different state governments and central governments have taken initiative to successfully implement E-Governance in various areas of services applying Information and Communication Technology (ICT) to provide better transparency, accuracy & security of its services to the citizens. In September, 2005, Parliament of India has passed the Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA), to enhance livelihood security by giving at least 100 days of guaranteed wage employment in a financial year to every house-hold in rural India. E-Governance solutions helps to simplify complex manual activities and supports transparent wage payment through agencies like Bank and Post-Offices. In e-governance, information's are exchanged between communicating parties via Internet and message may be changed, modified or destroyed by hackers during its transmission through Internet. So, information hiding is needed at the time of exchanging information via Internet. In this paper, we propose a tool, called Public-Key Watermarking algorithm, for integrity verification of Job-Card (JC) issued to individual house-hold by state governments, so that the watermark is capable enough to detect any changes made to the Job-Card by malicious users and can also identify fraudulent wage payment.***

Index Terms - ***E-Governance, Watermark-Insertion, Watermark-Extraction, Cryptography, Digital Watermarking, Public-key, Private-key, JC, ICT, MGNREGA***

1. INTRODUCTION

According to New Oxford English Dictionary, Government is the sum total of the systems by which a state or community is governed. The Government of India has specified e-governance as nothing but "using IT to bring about SMART (Simple, Moral, Accountable, Responsive, Transparent) governance" [1]. The benefits of e-governance suggest that it is convenient and cost-effective for businesses and government service deliveries. By supplying most current information in easier accessing way to public, the government can save energy, time and above all money. Another advantage of e-governance is greater citizen participation in government activities in environmental friendly way as number of paper exchange is very less compared to conventional system. Though in the modern times every government organizations are transforming their operations into electronic way, the implementation of e-governance also produces several risks which sometimes negate the advantages. One of the major risks of successful implementation of e-governance is security of information as all the important data about government and citizens and businesses are available online and anyone can freely access that information and if want can also change them easily.

The availability of large amount of information and increased use of multimedia across the Internet has become an effective way to provide services to people around the globe. The growing usage of multimedia content on the Internet generates several serious problems like fraud, forgery, counterfeiting, violation of copyright and piracy [8]. With the availability of new generation software and hardware, anyone can easily use the copyrighted material without being caught. In modern days, the transition from analogue and paper media to digital media has provided several benefits but also creates problems for the owner as the replicas of digital media cannot be distinguished from the original. To provide copyright protection of digital content, sometimes cryptographic approach is used but it does not completely solve the problem. To restrict unauthorized user from accessing copyrighted digital information, a new technology referred as watermarking have been developed. We can divide digital watermarking into two main categories: visible and invisible [8]. In visible digital watermarking, the information is visible in the content and is equivalent to stamping a watermark on paper. In invisible digital watermarking, information is added as digital data to content, but it cannot be indentified visually.

The Government of India (GoI), in September, 2005, has launched an ambitious project, named MGNREGA, with the hope to change the socio-economic [1] structure of the rural INDIA and all its citizens. The main purpose of MGNREGA [1] is to develop long-term rural infrastructure as well as to enhance living standards of the rural people. Under this act, Gram-Panchayats play a pivotal role for planning and implementation of different schemes. The size and coverage of the scheme demands a foolproof and secure system that can ensure that benefits flow only to them for whom it is intended [1]. So, we have developed a watermarking approach via which we can support privacy, integrity, and authentication related issues of digital documents and give confidence to the user of the document that the transmission process is secure.

In section-II, we have highlighted construction of Job-Card that may be used in ICT solution for MGNREGA scheme and section-III identifies basics of Public-key Watermarking

[1] *Lecturer, Department of Computer Science & Technology, Kanyapur Polytechnic, Asansol – 5, Burdwan, India*
[2] *Reader,Department of Computer Science University of Burdwan, Burdwan, India.*
E-Mail: [1]sirsendusarbavidya@gmail.com and [2]sunilkarforma@yahoo.com

technique. In section-IV, we have identified methods of incorporating watermark and its extraction techniques to provide authenticity of Job-Card in the light of proposed algorithm of the paper.

2. JOB CARD BASED E-GOVERNANCE

Under MGNREGA scheme, every rural family can register at Gram-Panchayats by filling a registration form that is kept under the supervision of village-head. Every registration related to wage seeker family will be sent to Computer Center (CC) at block level for higher-level processing.

For every valid application, CC will assign an ID comprising a 15 digit unique registration number. This registration number contains two parts – 11 digit code containing district, assembly, block, Panchayats, and village information and 4 digit index number for individual family.

After generating the unique registration ID for every wage seeker family, the CC will create a Job-Card and affix a scanned image of the job seeker family in the designated space within the Job-Card and will handed it over to the Gram-Panchayats for delivery of the same to the corresponding wage seeker family. The wage seekers can directly draw cash from paying agencies as per the wage list, by showing Job-Card and providing a thumb impression.

Here comes the necessity of public-key watermarking [3] technique, which not only restrict the fraudulent wage payment but also guarantees that paying agencies are not able to develop their own wage list.

The whole application can easily be fitted into Government-to-Citizen (G2C) model, where government portion of the application is responsible for the creation, distribution and processing of the Job-Card and Citizen portion is only responsible for providing necessary information.

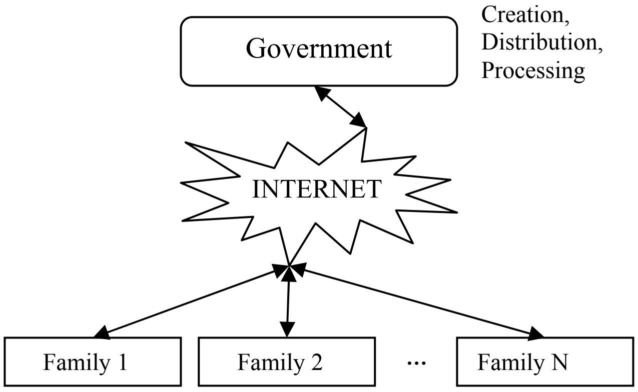

Figure 1: A G2C Model

The parameters included in the Job-Card are shown in the figure 2.

The registration process in the MGNREGA scheme is described with the help of the figure 3.

3. A G2C MODEL USING PUBLIC-KEY WATERMARKING

Digital watermarking [5] is used to insert a digital signature into the content so that the signature can be extracted for the purposes of ownership verification and/or authentication. Digital watermarking is a way to protect ownership property from illegal usage. A watermark always resides permanently within the host information. The watermark is hidden in the host data in such a way that no one can separate it from the original work but the work is still accessible.

JOB CARD REGISTRATION NUMBER (15 DIGIT)		
DISTRICT	(2 DIGIT)	PASTE PHOTO HERE
ASSEMBLY	(3 DIGIT)	
BLOCK	(2 DIGIT)	
PANCHAYAT	(2 DIGIT)	
VILLAGE	(2 DIGIT)	
FAMILY INDEX	(4 DIGIT)	

Figure2: Schematic representation of Job-card mentioning different parameters

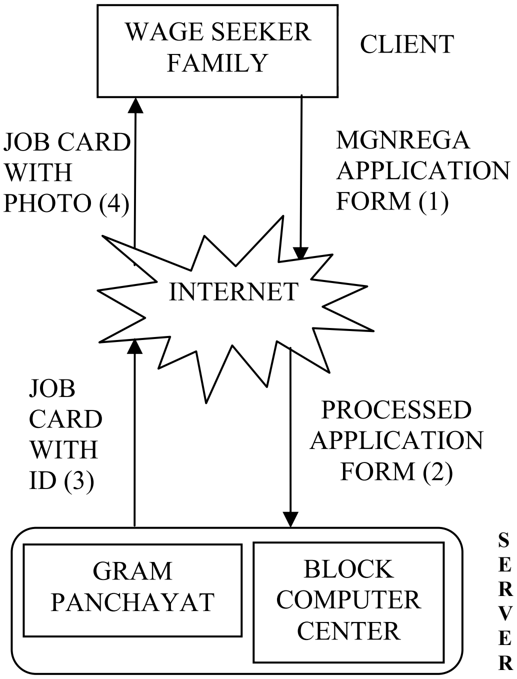

Figure 3: Registration Process in MGNREGA Scheme

It inserts the hidden information into the content, also called the cover-media [6]. This hidden information is called the watermark. After inserting the watermark via specific algorithms, the original media will be slightly modified and is referred as watermarked media. There might be no or little perceptible differences between the original media content and the watermarked one. After embedding the watermark, the watermarked media are sent over the transmission channel to the receiver, where they are checked for authenticity of the content owner. A technique called watermark extraction [10] is performed here for verification of the ownership. The watermark information is fully depends on the application type. The generalized algorithm of watermarking is described below.

Step 1: Initially, select a cover media.

Step 2: Insert hidden information (watermark) into the content (cover media).

Step 3: After watermark embedding, the watermarked media is sent to the receiver via transmission channel.

Step 4: Watermark extraction approach is applied at the receiver end to identify the authenticity of the owner.

Watermark embedding and detection can sometimes be considered analogous to encryption and decryption in cryptography. There are two types of cryptographic approaches that we can use in watermark applications – Secret-key approach and Public-key approach.

In Secret-key watermarking, we have an embedding function that takes a message, an original work and outputs a watermarked work. Similarly, we have a detection function, which takes a watermarked work and outputs a message. The mapping between watermarked works and the messages is controlled by a watermark key. Watermarking algorithms based on a Secret-key present a major drawback; they do not allow a public recovery of the watermark. In order to overcome this limitation, Public-key watermarking algorithms have been proposed; such systems consist of two types of keys: a public and a private one. Content can be watermarked using the private key, whereas the public key is used to verify the mark.

We might develop a Public-key system, so that knowledge of either key does not allow an adversary to find out the other key. The public key can be widely distributed without risk of giving away the private key. Depending on the application, either the encryption key or the decryption key can be public.

The description of Public-key allows feasible computation of the mapping in only one direction. To implement Public-key watermarking, the watermark embedding use one watermark key and the watermark detector use a different watermark key. The assumption is that knowledge of the detection key is not sufficient to allow an adversary to remove a watermark.

4. PROPOSED ALGORITHM

In our approach, we use two types of keys, one is Public-key (E) for Watermark-Insertion within the information present in Job Card (JC) and the other is Private-key (D) for Watermark-Extraction from the watermarked message. Encryption and Decryption method both use MODULAR_EXPONENTIATION [3] technique and the modulus n, a very large number (256 bits) is created during the key generation process by using conventional RSA algorithm [3].

a) **Key Generation Algorithm**: Using this algorithm, we generate two types of keys that are used in the watermarking application. This process actually executed in the Government side (Computer Center) of the G2C model.

1. Using conventional RSA algorithm, we find e, n and d, where e is public exponent, d is private exponent, and we choose, the modulus n, a very large number (256 bits) for the purpose of better security.
2. Then we apply ITERATED HASH FUNCTION [3] on the original information present in Job-Card using the generated e and d and generate corresponding Public-key (E) and Private-key (D).

b) **Watermark Insertion Algorithm**: This algorithm is developed to insert generated watermark in the original information present in the Job-Card to provide security and authenticity. This process is also executed in the Government side (Computer Center) of the G2C model.

1. Let, M_k denotes the kth block of data [7] within the message I.
2. Let, H (.) be a Cryptographic Hash Function such as MD5 [3]. We compute H (M_k, E) = $(m_1, m_2, \ldots, m_s)^k$, where s is the size of MD (message Digest) [In our algorithm, we have chosen the minimum length of s is 256 bits].
3. Finally, we encrypt the generated result of individual blocks with encryption function E (.) using the public key E to produce the corresponding watermarked block M_k'.

Here, in watermark insertion process [9, 12], the input to the scheme is the watermark (unique Job-Card registration number), the cover-media (Job-Card) and a Public-key (generated using our proposed algorithm). The Public-key is used to enforce security, which is the prevention of unauthorized parties from recovering and manipulating the watermark. The output of the watermarking scheme is the watermarked Job-Card, which will be distributed to the wage seeker families via Panchayats.

Here, we achieved a better security by applying multiple keys to the information of the Job-Card. Before watermarking, we encrypt the information using some encryption keys and then apply watermark information on that encrypted information. In this way, use of two different keys allow us to provide better security as no one can interpret the actual hidden information until and unless they possess both the keys.

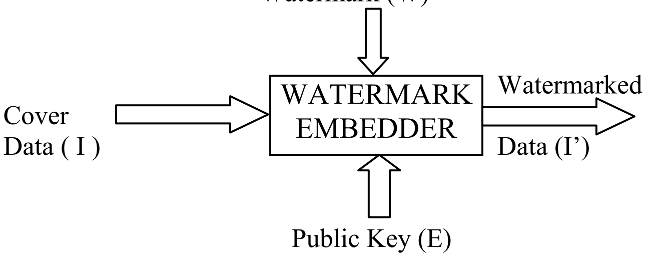

Figure 4: Digital Watermark Insertion Scheme

c) **Watermark Extraction Algorithm**: This algorithm is developed to extract generated watermark from the watermarked information in the Job-Card to identify authenticity of the message. This process is executed in the client side (Bank, Post-Offices) of the G2C model.

1. We split the watermarked message I" into s number of blocks.
2. Apply a decryption function D (.) on individual blocks M_k' using the private-key D to produce the corresponding block M_k of watermarked message I".
3. Finally, we apply the same Hash function, which is used to encrypt the message, on M_k to produce the final message using private-key D and generate authenticity information about the message as final outcome.
4. Depending on the generated authenticity information, the Job-Card will either be accepted or rejected.

In Watermark extraction process [2, 4, 11], inputs to the scheme are the watermarked data, Private-key (generated by the same proposed algorithm that are used to develop public key), and the original watermark. The output of the scheme gives us some kind of confidence measure indicating whether the test data is authentic or not.

Here, we achieved better security by using multiple keys at different levels of application. Initially, watermark is extracted from the information of the Job-Card using watermark key and successful extraction of which actually guarantees the authenticity of the owner. Then we apply decryption key to the authenticated information to produce the actual information from the encrypted information. In this way, two tier applications of keys provide a better hiding of valuable information from the intruders and only knowing of both the keys actual help to extract the information from the Job-Card. Thus the security measurement is very high if we use the above mentioned approach.

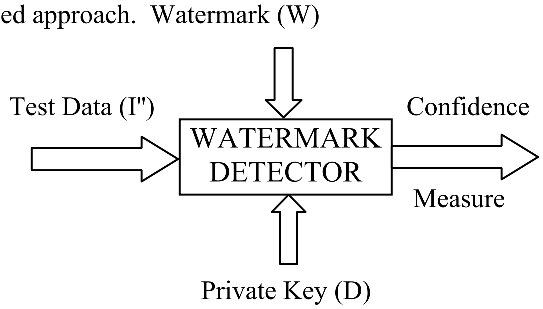

Figure 5: Digital Watermark Extraction Scheme

5. CONCLUSION

Here, we have used a public key for watermark insertion and a private key for watermark detection. So, any person can perform the authenticity check by simply using a private key and a watermark detector device. Though the approach specifies a direct relationship between Watermarking and Cryptography, there are some fundamental differences exists between them. In Public-key Watermarking, the mapping between Job-Card and information's within the Job-Card are many-to-one, so that given information may be embedded in any given Job-Card. On the other hand, in Public-key Cryptography, the mapping between cipher-text and plain-text is always one-to-one.

Our approach combines the advantages of both Watermarking and Cryptography and produce a robust system to keep secure information hidden from the intruders. At the time of Job-Card production, we apply both cryptographic and watermarking approach and at the time of extracting information from that Job-Card, we again apply both cryptographic and watermarking approach, but the order of applying them is reverse in this case. The proposed approach is robust enough to protect against any kind of malicious attack performed by intruders. Any changes made to either the Job-Card or to its information, can easily be detected and thus the purpose of security is maintained.

FUTURE SCOPE

The Public-key algorithm stated here requires much more computation than Secret-key algorithm. It is impractical to encrypt and decrypt large messages using the above method. So, it is common to use a Secret-key algorithm for transmission of large amounts of data and to transmit its key, we need to use a Public-key algorithm. As the space in all the contents where watermarking techniques can be useful is very limited, it is impossible for us to use many kinds of watermarking techniques for some applications ambitiously. Our proposal is that, prior to application of watermark information compress the whole data using any compression algorithm. In this way we can reduce both the computation time as well as storage requirement.

REFERENCES

[1]. Agarwal A. - E-governance: Case study, Hyderabad: University Press, 2007.

[2]. Fabien A. P. Petitcolas and Ross J. Anderson, "Evaluation of copyright marking systems," Proceedings of IEEE Multimedia Systems'99, vol. 1, pp. 574-579, 7-11 June 1999, Florence, Italy.

[3]. Forouzan B. A. - Cryptography and Network Security: (Special Indian Edition), New Delhi: Tata McGraw Hill, 2007.

Continued on page no. 444