Reduction of fragile watermark computational complexity by use of AES encryption

Reddy Kamal Teja Gurramkonda, Hadassah Pearlyn Nagathota
School of Telecommunication
Blekinge Institute of Technology
Karlskrona, Sweden
kamalteja1993@gmail.com,hadassahpearlyn7@gmail.com

Dawid Czekajski, Wlodek J. Kulesza
School of Engineering
Blekinge Institute of Technology
Karlskrona, Sweden
dawid.czekajski@gmail.com, wka@bth.se

***Abstract*—Fragile watermarking is an authentication technique for identifying any manipulations in the digital media. The existing fragile watermarking scheme uses RSA encryption algorithm to ensure security of the watermark from malicious attacks. In this paper, a new scheme is proposed where RSA algorithm is substituted with AES algorithm to reduce computational complexity (thus making it easier and more economical) without compromising its safety. Both existing and proposed schemes are implemented in Matlab software suite and their complexity (measured in average operation time) is compared while the security issue is discussed on theoretical grounds according to strengths and weaknesses of encryption algorithms.**

Index Terms—Digital media, Encryption, Security

I. Introduction

Amount of digital content like images, videos and audio files uploaded into the internet is growing steadily. Much of it is copyrighted in some way and therefore needs protection from illegal activities like copying and tampering. One method of protection is to embed digital watermarks directly into the media files. There are two distinct types of digital watermark — robust and fragile. Robust watermark is designed to resist any type of potential image modification in order to keep metadata embedded into it intact. Fragile watermark is supposed to change with any tampering in a way which allows to determine exact place of the modification. However, the watermark itself is vulnerable to multiple types of attacks meant to remove or disable it and needs to be secured with some type of encryption [1].

Enormous number of files are being processed by big datacenters daily. Constant growth in volume of digital content circulating through the web needs to be accompanied by improvement of technologies used to protect the content and its owners from mishandling of intellectual property. So, there is a need for implementation of better and faster algorithms as well as maintaining reasonable level of security.

One example of fragile watermarking scheme using RSA encryption technique was presented by Hajime Kubota and Keiichi Iwamura [2]. According to our research the best field for improvement lays in the encryption methods used to secure watermarking schemes. We modified their solution, substituting RSA with AES technique to reduce entire scheme computational complexity without compromising its security.

II. Survey of Related Works

The paper contains important basics about the concept of watermarking, various types of watermarks and their corresponding vulnerabilities [1].

The authors evaluate numerous fragile watermarking schemes from the standpoint of their security finding faults with each one and proposing their own solution using RSA-OAEP encryption technique because of its acclaimed resistance to most of the cryptographic attacks. Proposed scheme was used as a base for our work [2].

Comparison of three popular encryption techniques**—**RSA, DES and AES from the standpoint of their speed and security is analysed. Although the security analysis seems lacking and need to be supplemented with additional research results, the speed tests are conclusive and prove that AES algorithm is much faster when compared to others. AES is proven to be secure against practically possible types of attacks. The use of 256-bit key helps encryption time to be much faster than other algorithms of which RSA is one of the slowest [3]. Implementation of AES algorithm in Matlab suite is described briefly [4].

III. Problem Statement and Main Contribution

Solution presented in [2] is very secure against most types of attacks. Its problem is high computational complexity caused by use of highly complex RSA-OAEP algorithm. Encrypted media is divided into a large number of individually processed blocks, due to which the time needed for the encryption of each one sums up and starts to be noticeable in case of large, high-resolution images or high-fidelity audio/video files. Can the fragile watermarking schemes using another type of encryption be less computationally complex and at least comparably secure to existing schemes? The hypothesis is that AES encryption algorithm can be substituted instead of RSA in the watermarking scheme resulting in lowering its total complexity. AES-256 is also proven resistant to all types of known attacks**,** complexities of the attacks are prohibitively high enough for them to be impractical which ensures at least comparable security standard.

The main contribution of this paper is implementation of two watermarking schemes one using RSA-OAEP and second using AES in the form of Matlab code and comparison of time required by them to process the stock image.

IV. Problem Solution

A. Modeling

The image is watermarked and encrypted using chosen encryption method. The scheme works by dividing the processed image into blocks, calculating hash values for each block, constructing the stamp image including information for RSA and then encrypting the data.

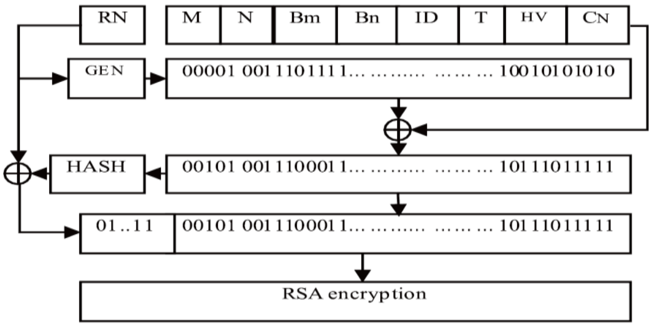

Fig. 1. Process of watermarking with RSA-OAEP encryption

System follows the algorithm as depicted in the Fig.1.

TABLE I
VARIABLES IN THE ALGORITHM

Variables	Description
M x N	Size of the original image.
m x n	Size of the rectangular block
B_m , B_n	Block coordinates.
HV	Hash value of all pixels in each block generated by SHA-256 function.
ID	Image index given by *ID* of embedding machine and T which is differed for every block.
T	Generation time of the watermark.
CN	Constant number that can be decided by either the user or service.
RN	Random number generated by the pseudo-random number generator.
GEN	Pseudo-random generator using seed RN
HASH	Hash function to generate a hash number

Firstly, at the lower and right end of the image, if needed, additional pixels are padded in order to divide it into equal blocks. Secondly, in order to make it pseudorandom, the message is padded using OAEP technique**. T**he random number which is generated (RN) and the watermarking information whose size is 1024 bits are given as inputs to EXOR function. Then, the obtained EXOR result is given as input to the HASH function. Taking the result from the HASH function and RN as inputs, EXOR operation is performed again. The result attained is then attached to the first EXOR result. The RSA encryption technique is applied to both the EXOR results. The LSB of the block is replaced by the calculated digital signature.

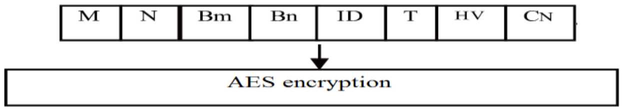

Fig. 2. Process of watermarking with AES encryption

Upgraded scheme as shown in Fig.2 employs AES instead of RSA-OAEP encryption technique.

B. Implementation

The small key versions in RSA-OAEP like 64,128,256 bit keys and AES schemes are implemented as described in previous section. Implementation of RSA-1024 requires storing of large prime numbers in Matlab but the base version of Matlab has design limitations and the data is truncated.

Matlab function for AES encryption is adapted and its process is much simpler because AES encryption does not need additional message padding as for RSA. AES-256 is used. Firstly, image of dimensions 195 X 259 and size 15.3 KB is processed by dividing it into equal sized blocks, removing the least significant bit of each pixel in each block and creating its hash function with SHA-256. Secondly, the processed block is represented as a matrix which is given as input to hash function. The output obtained is a hexadecimal hash value which is converted to binary. Using this block data, watermark is created which is otherwise called as stamp image and is encrypted to make it secure. It is then embedded into LSB's of each pixel of each block.

C. Validation and Verification

The time needed to process a stock image is calculated. Mean times needed by computer equipped with 1,7GHz processor to successfully process a 195 X 259 pixel monochromatic image are measured and are tabulated in TABLE II.

TABLE II
MEAN TIMES OBTAINED

Part	Mean Time
Image Processing	82 sec
Processing with OAEP padding	92 sec
Full AES scheme	108 sec

This means AES encryption took around 26 seconds. Time consumption by RSA would have to be shorter than 10 seconds to compete with AES which, based on our knowledge of the algorithm, is impossible.

V. Conclusions

The main conclusion is that AES is superior to the RSA in this application and the encryption time is about 20% of total time needed to embed the image with a watermark. Potential enhancement of security connected with updating the encryption technique is also of value, 1024-bit keyed RSA is already breakable and in coming years its security standard is expected to decrease while AES is believed to be resistant to attacks for a reasonable amount of time.

Future work could be further research on watermarking techniques and other image processing technologies like DCT, devising a more efficient solution not relying on processing of the entire image. Although encryption did not prove to be main computational problem in watermarking scheme further research in the encryption techniques and determining the optimal one would also contribute in improving the simplicity and efficiency.

References

[1] J. Nin and S. Ricciardi, "Digital watermarking techniques and security issues in the information and communication society," in *27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013, March 25, 2013 - March 28, 2013*, 2013, pp. 1553–1558.

[2] H. Kubota and K. Iwamura, "A new fragile watermarking scheme and its security evaluation," in *2010 7th IEEE Consumer Communications and Networking Conference (CCNC), 9-12 Jan. 2010*, 2010, p. 5 pp.

[3] P. Mahajan, A. Sachdeva, and Dr, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Glob. J. Comput. Sci. Technol.*, vol. 13, no. 15, Jul. 2013.

[4] J. J. Buchholz, *Matlab Implementation of the Advanced Encryption Standard*. Dec. 19, 2001: buchholz.hs-bremen.de.

Dawid Czekajski was born in Kwidzyn, Poland in 1991. He received the B.S degree in control engineering and robotics from Gdansk University of Technology in 2013. He is currently pursuing the Double Diploma programme including M.S degree in signal processing at Blekinge Institute of Technology and M.S degree in control engineering at Gdansk University of Technology.

During the summer of 2012 he worked as Intern with Energa Operator, one of the biggest electricity providers in Poland and during the summer of 2014 he completed an internship in ASTOR, one of the leading Polish companies in the field of control engineering, industry automation and robotics.

Mr. Czekajski is not a member of any professional societies yet.

Reddy Kamal Teja Gurramkonda was born in Hyderabad city, India, in 1993. He has completed his Bachelor of Technology (B.Tech) in Electronics and Communication Engineering (ECE) as major, in the year 2010-2013 from Jawaharlal Nehru Technological University (JNTU). He is currently pursuing Master of Science (MSc) having major study in the field of Telecommunication systems in Blekinge Tekniska Högskola (BTH).

He was the project leader in Bachelors project titled "***Active tag Based Assert/Personal Tracking"*** in the year 2013. He did his B.Tech project in a company named ***Austria Micro Systems*** (AMS) using **"*Active tag and GSM technology"***. His research interests include network virtualization.

Mr. Reddy Kamal Teja Gurramkonda was awarded a certificate for his paper presentation on **"*GSM and GPRS Technology"***.

Hadassah Pearlyn, Nagathota was born in Vijayawada, India in the year 1993.She completed her Bachelors degree in the field of electronics and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India in the year 2013.She is pursuing her Masters degree in the field of telecommunication systems from Blekinge Institute of Technology, Karlskrona, Sweden.

Her bachelors thesis is based on RFID which is titled "Active Tag Based Personnel/Asset Tracking" using low frequency reader in Austria Micro Systems(AMS),Hyderabad, India. Networking is her field of interest in which she wants to research.