VERSITA

ANNUAL OF NAVIGATION 19/2012/part 2

10.2478/v10367-012-0014-8

BARTOSZ CZAPLEWSKI
Gdansk University of Technology

KRZYSZTOF CZAPLEWSKI
Polish Naval Academy

PROTECTION OF VISUAL DATA TRANSMISSION FOR VESSEL TRAFFIC SYSTEMS USING JOINT FINGERPRINTING AND DECRYPTION METHOD BASED ON MODIFIED HILL CIPHER

ABSTRACT

Vessel traffic systems provide a high level of safety on coastal waters due to coastal radar stations and industrial cameras transmitting information to traffic supervision centers, as well. To improve a vessel traffic services is very important to ensure the speed and secrecy for the transmission of video images.

The paper presents the basic issues of the multimedia data protection by digital watermarking and fingerprinting methods. Main applications for such digital marking were described in the paper as well as its requirements. Furthermore, the importance of multicast transmission for fingerprinting methods was presented by comparing the scalability of methods using only unicast transmissions and methods using multicast transmissions. The paper also presents the greatest threat to fingerprinting methods, which are attacks performed by more than one pirate. These attacks are called collusion attacks. The criteria that should be followed during identifying rogue users taking part in the collusion attack on the security systems has been presented.

The paper also contains description of the extended Hillcast method, which belongs to the group of JFD (Joint Fingerprinting and Decryption) methods. The method provides a cryptographic security and digital fingerprinting of multimedia content, while maintaining high scalability. Main purpose of this method is VoD (Video on Demand) service, but it can also be used in vessel traffic supervision systems, such as VTS and AIS. In the last part of paper, there are results of studies which indicate high resistance to most common collusion attacks. Method proposed by authors can enhance the security of visual data transmission in vessel traffic systems.

Keywords:
data protecting, VTS, fingerprinting, Hill cipher.

INTRODUCTION

The usage of industrial cameras in VTS systems not only provides maritime safety and marine environment protection, but also protect ships against raids. This is done by transmitting the video image in real time, which allows for immediate response by the marine traffic controller. Obviously, video content should be accessible only by authorized service. It can be achieved only if the transmission is properly secured, which can be done physically or in software. Physical security, which would involve permanent monitoring of the transmission line, would be expensive and limited to the wired network. Therefore, it is worth to look at software security of transmitted multimedia data.

There are two complementary methods for multimedia protection and copyright [5]. First method is an encryption, which main objective is to ensure confidentiality of the transferred media. Encryption provides that only registered users with proper decryption keys will be able to decrypt information and use it. Unfortunately, encryption isn't sufficient protection, because after decryption, user with access to the content may easily violate copyright by making decrypted data available to public without permission.

Addition to encryption is second method called a digital fingerprinting. Digital fingerprinting methods rely on embedding of some secret additional data into multimedia. This data, called a fingerprint, uniquely identifies the transmitting or receiving side and it remains unnoticed. There is a possibility of further analysis of a intercepted copy which is suspected of being illegally shared. Purpose of such analysis is to determine by whom a copy has been illegally shared. This information may be basis for further and more detailed observations or even accusations of unfair users and bringing them to justice.

REQUIREMENTS AND APPLICATIONS

While designing fingerprinting system, it's necessary to achieve a compromise between the three requirements [5], which are: imperceptibility, resistance to attacks and the maximum length of the embedded sequence. Imperceptibility is important because fingerprints cause some changes to the original signal, while a publisher wants to perceptual quality of multimedia remained unchanged. Thus, it is necessary to maintain the level of introduced changes below the level of noticeable changes to the human eye. Resistance to attacks is crucial, because even the best fingerprint won't accomplish its goal if it doesn't survive the attacks carried out by rogue users, called pirates. The last requirement is the maximum possible length of the fingerprints.

There are five main applications for digital watermarking and fingerprinting methods: protection of intellectual property (embedded data identifies the transmitting side and prevents from falsifying the identity of the source), authentication and manipulation detection (embedded long sequence of bits is used in later analysis aimed at verifying the integrity of the protected copy), access control (watermark carries information about the access to data), annotation (embedded data doesn't directly contribute to the copyright protection, but it's a tool to transmit additional hidden information) and digital fingerprinting, which is subject of this paper.

In this application, fingerprints are embedded in multimedia in order to identify users who violate copyright by creating and sharing illegal copies. The presence of digital fingerprint in a illegal copy is an evidence of crime committed by the user. Pirates will seek to remove their own fingerprints from marked copy. Therefore, the most important requirements for this type of application are resistance to attacks and imperceptibility.

FINGERPRINTING AND MULTICAST

For the distribution is important that the transmission cost of a single copy is as low as possible. Thus, in order to minimize costs, a transmitting side must provide a service for the maximum number of users with limited available bandwidth and computing resources. Furthermore, it is desirable to easily add or remove selected users during system operation. Multicast transmission solves all these problems.

However, the implementation of fingerprinting systems based on multicast transmission is problematic, because the goals of fingerprinting and multicast seem to be the opposite. Fingerprinting systems require that each user gets a different, uniquely marked copy, while the multicast transmission is a transfer of one, exactly the same, copy to all users. For this reason, multicast can't be applied directly to classic fingerprinting systems, because the uniqueness of each copy won't be retained.

Consider a situation when fingerprinting is using only unicast transmissions, as shown in figure 1. Transmitting side must generate fingerprints and then place them in copy for each user individually. There are as many marked copies as there are registered users. Each of these copies is individually encrypted and sent to users via unicast transmission. Receivers can use their copies after decryption. Please note that the encryption is not part of the fingerprinting method. In case of collusion attack, the distribution side intercepts a pirated copy, extracts the fingerprint and identify pirates.

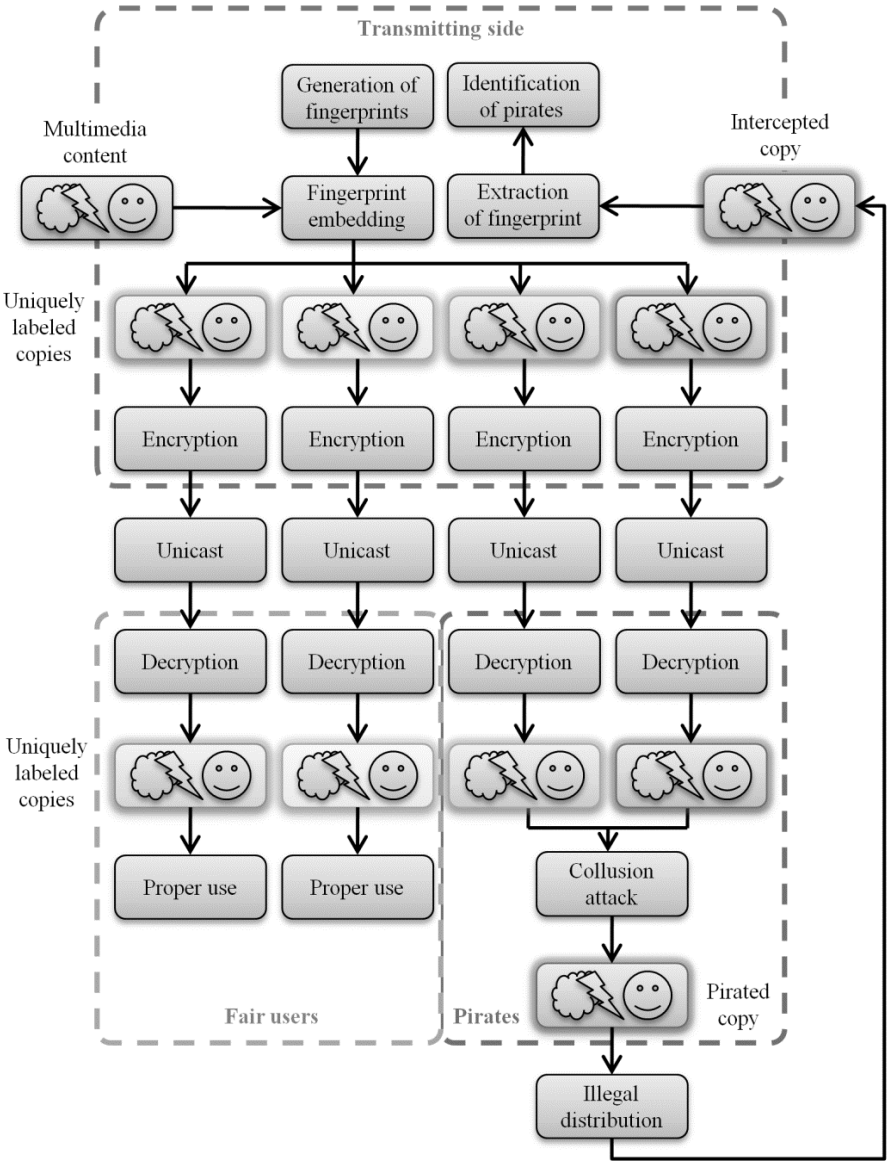

Fig. 1. Fingerprinting method implemented using unicast transmissions [own study]

This solution is poorly scalable for several reasons. The number of calculations that would make the distribution side would grow linearly with the number of users, which is a great disadvantage. Also, the available bandwidth would be inefficiently used, because total bandwidth required to provide a service to all users would be a multiple of bandwidth required to provide a service for one user. In this case, there

are multiple streams sent over the network, which are very similar, because fingerprints are embedded so as to remain unnoticed. Such a strategy leads to a waste of bandwidth.

There are many fingerprinting methods using multicast transmission, but the most promising are Joint Fingerprinting and Decryption methods (JFD) [1, 2, 4, 6]. An example is shown in figure 2.

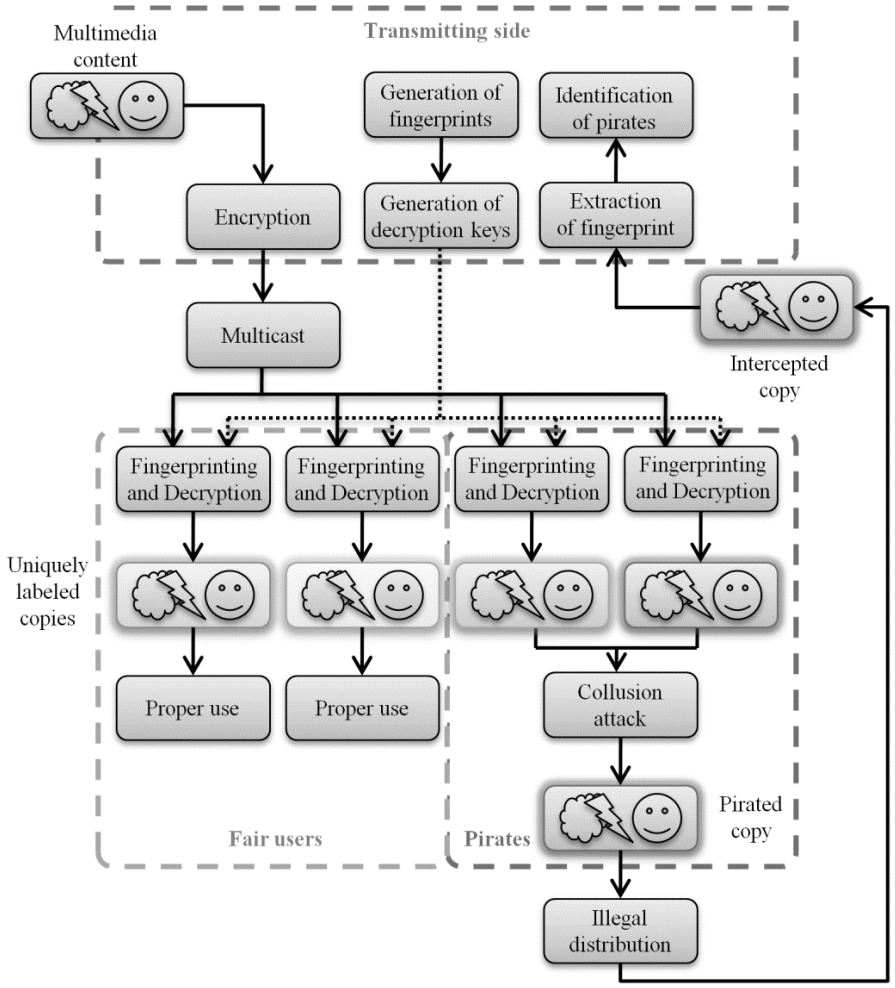

Fig. 2. Fingerprinting method implemented using multicast transmission [own study]

Embedding process is realized at the receiving side, so that distribution side doesn't have to perform many complicated operations. Only one copy of data is

encrypted using common group key. This copy is sent through multicast transmission to all registered users, so that bandwidth required to work the system and the number of connections is kept constant and independent of the number of customers. There is also a set of unique decryption keys for each user, which are sent to them through unicast transmissions. Unlike the previous strategy, encryption is a integral part of the fingerprinting method. Decryption keys are constructed so that decryption introduces changes in media. These changes are unique for all the users and are imperceptible to the human, so these changes are fingerprints. The receiving side is also not burdened with additional operations because fingerprinting is performed during the decryption process. These properties provide high scalability, which is extremely important in multimedia distribution systems.

COLLUSION ATTACKS

Currently the biggest threat are collusion attacks, where pirates cooperate with each other. Users with differently marked copies of the same content can work together by examining the copies available to them and make effective attacks on the fingerprints. As a result of such attack a pirated copy without fingerprint or with fingerprint not associated with the pirates involved in the collusion is obtained.

Linear collusion attack is a type of collusion attack, which is mostly used by pirates. In linear collusion attack, many users combine copies available to them in such linear function [5]:

$$p = \sum_{i=1}^{h} \lambda_i \cdot x_i, \tag{1}$$

where h is the number of colluded users, x is a marked signal of i-th user, p is a pirated copy obtained in the attack and λ_i is weight coefficient assigned to the i-th user. If weights are equal for each user, than this is a collusion attack by averaging. Linear collusion attack by averaging doesn't reduce the visual quality of multimedia content. Furthermore, according to [3, 8], collusion attack by averaging can be successfully used to model many other, even non-linear attacks.

In order to identify the pirates, fingerprints of individual users are compared to fingerprint extracted from the suspicious copy. Usually this is done using the correlation function or correlation coefficient and it is necessary to define a detection threshold. If the correlation of fingerprints for specific user is greater than the threshold, the user shall be deemed guilty of piracy. Detection threshold should be chosen in such a way that the fingerprint system meets certain criteria. There are three possible strategies that can be followed to detect pirates [7].

First strategy is to detect at least one dishonest user. Threshold is chosen in such a way that the probability of detection at least one pirate was as high as possible, with the assumed very low probability of false accusation of an innocent user. The aim is to detect some of the pirates without the risk of accusations of innocent. This is particularly important in gathering evidence.

Another strategy is to detect many pirates. Probability of detecting most of the pirates is high, at the expense of greater likelihood of unjust accusations of innocent users. Compared to the previous scenario, this one accepts the possibility of prosecution of several innocent users for the benefit of detecting a greater number of pirates. The result is a group of pirates who have been properly detect and innocent users who have become suspects, so further investigation is needed.

Last strategy is to detect all the pirates. Threshold is chosen in such a way that the probability of detecting all of the pirates is very high and probability of false accusation of an innocent user is at a acceptable level. The aim is to detect all the pirates and measure of performance is the ratio of the average number of wrongly accused users per one pirate. It is applicable in cases where the transmitted data is a matter of great importance and safety, and there is a need to detect all the people involved in the crime at any cost.

METHOD DESCRIPTION

For research purpose, the Hillcast method [6] has been chosen. In order to simulate a distribution system, the method had been implemented in the following manner. Image (plaintext) **X** and ciphertext **Y** are square matrixes of size n x n. Since a single video frame isn't usually square, so sub-image will be encrypted. This is not a significant obstacle, because we avoid the encryption of full video frames in order to avoid high complexity. Location of encrypted fragments can vary randomly according to the algorithm that must be known to the receiver.

Ciphertext **Y** is obtained by multiplying the image matrix **X** by an encryption key matrix **E**:

$$\mathbf{Y} = \mathbf{XE} \; mod \; 256, \tag{2}$$

where all three matrixes are of size n x n and elements of these matrixes have values from 0 to 255. The key matrix **E** must be modular invertible.

The decryption key **D** must be associated with the receiver's unique fingerprint **F** in the following way:

$$\mathbf{D} = \mathbf{E}^{-1}(\mathbf{I} + \alpha\mathbf{F}), \tag{3}$$

where α is embedding strength coefficient and **F** is a matrix containing a fingerprint and it's unique cross all users. The matrix $\mathbf{E}^{-1}$ is the modular inverse of the matrix **E**. The value of the coefficient α depends on the length and type of used fingerprints and it should be chosen experimentally In such a way to maintain fingerprint's imperceptibility while obtaining the greatest possible resistance to attacks.

After receiving the ciphertext **Y**, the receiver uses his key **D** to obtain a marked copy $\mathbf{X_D}$. Joint fingerprinting and decryption is performer according to the formula:

$$\mathbf{X_D} = \lfloor \mathbf{YD}\ mod\ 256 \rfloor, \tag{4}$$

while formulas (2) and (3) implies:

$$\mathbf{X_D} = \lfloor \mathbf{XEE}^{-1}(\mathbf{I} + \alpha\mathbf{F})\ mod\ 256 \rfloor = \lfloor \mathbf{X} + \alpha\mathbf{XF}\ mod\ 256 \rfloor. \tag{5}$$

The extraction of fingerprint from the intercepted copy $\mathbf{X_{TEST}}$ is realized by a distribution side with coherent detection. The extraction may be conducted using the following formula:

$$\mathbf{F_R} = \frac{1}{\propto}(\mathbf{X_{TEST}} - \mathbf{X}), \tag{6}$$

In order to detect pirates, we must examine correlation between the extracted matrix of real fingerprint $\mathbf{F_R}$ and a product of matrixes **XF** because, as it is clear from formula (5), this is a matrix embedded in the image.

RESULTS

In order to present the performance of the method, authors simulated series of attacks and detections. In the simulated system, there are 200 receivers of visual information and each of them receives a marked data with fingerprint of a length of 4096 symbols. Two groups of simulations were conducted: one for fingerprints with random values normally distributed and one for orthogonal fingerprints from Hadamard matrix.

Simulations used four images presented in figure 3. Every image is the size of 256 by 256 pixels in grayscale. In any case, an encrypted data was only a sub-image of size 128 by 128 pixels randomly positioned in the whole image, which is shown in figure 4.

For each set of marked copies 10 collusion attacks were performed. All attacks were attacks by averaging with a different number of pirates: 3, 6, 9, 12, 15, 18, 21, 24, 27, 30. After collusion attacks, detection process was performed for different correlation thresholds. For each type of fingerprint a different set of correlation thresholds was used . Each scenario was repeated 20 times and results presented in figures 5 and 6 are the average value.

The simulation results for all sample images were almost the same, so only a few selected plots are presented. It can be observed that by using not orthogonal fingerprints, the detection of pirates drops fast. The number of detected pirates depends on the chosen threshold. For example, in fig. 5., if there are 15 pirates, method is able to detect only half of the pirates (~50%) for threshold 0,65. At the same time, if orthogonal fingerprints are used, detection of pirates remains at the same level and even if there are 30 pirates, method can detect most of them, as shown in fig. 6.

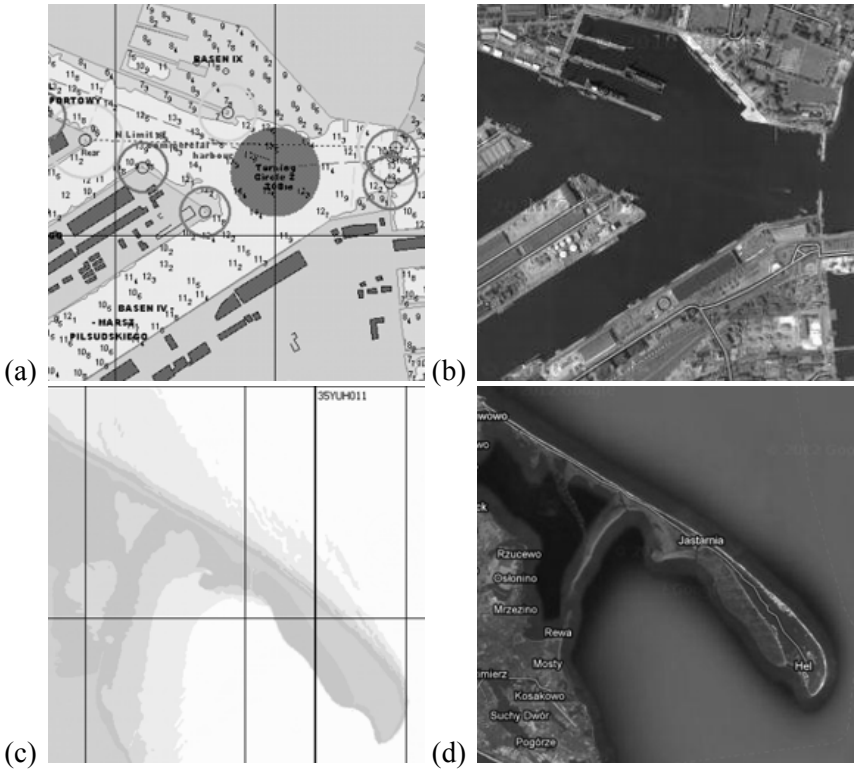

Fig. 3. Sample images used in simulations: (a) map1.bmp; (b) sat1.bmp; (c) map2.bmp; (d) sat2.bmp [own study using NTPro 5000 and Google Maps]

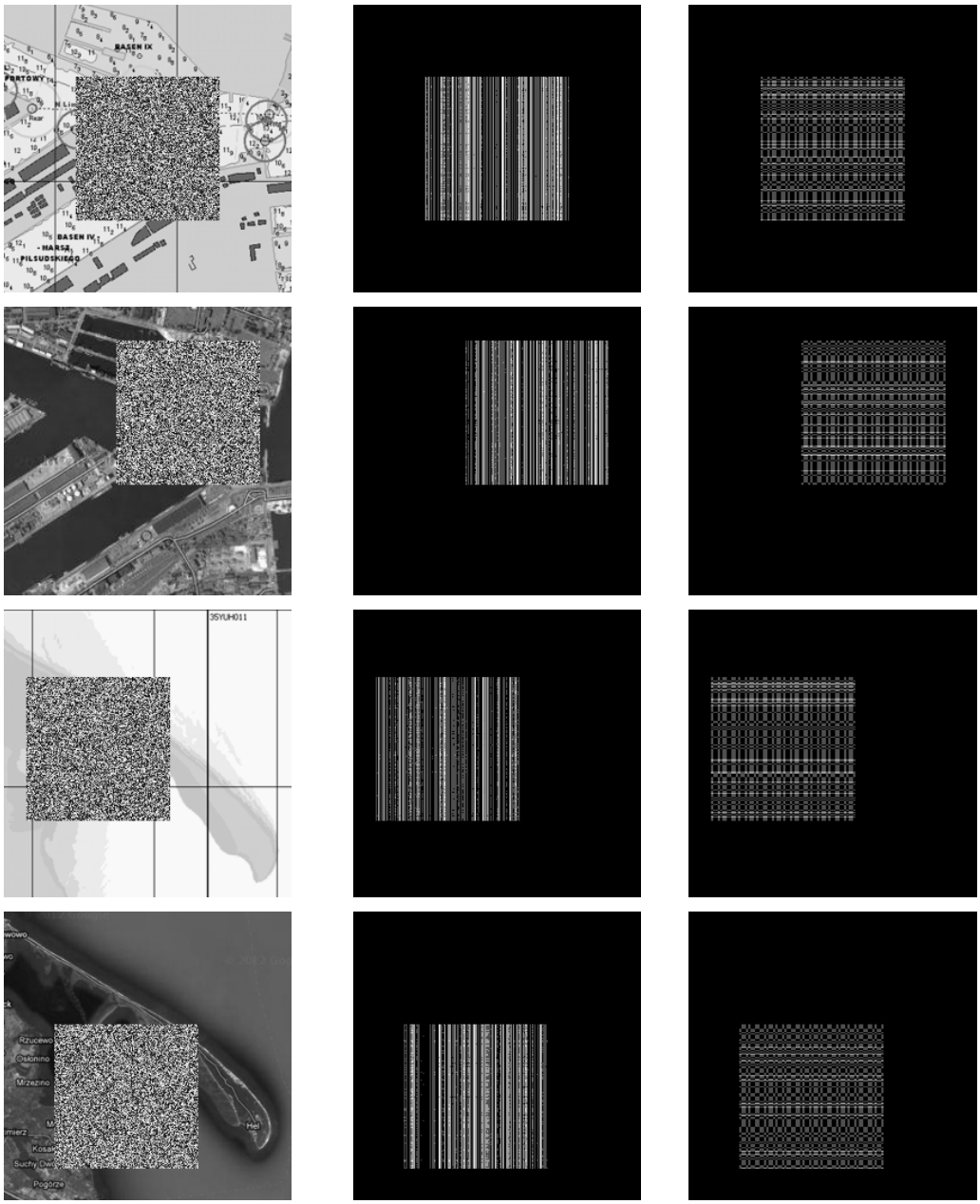

Fig. 4. Encrypted images (left column), extracted fingerprints with random values normally distributed (middle column) and extracted orthogonal fingerprints from Hadamard matrix (right column) [own study]

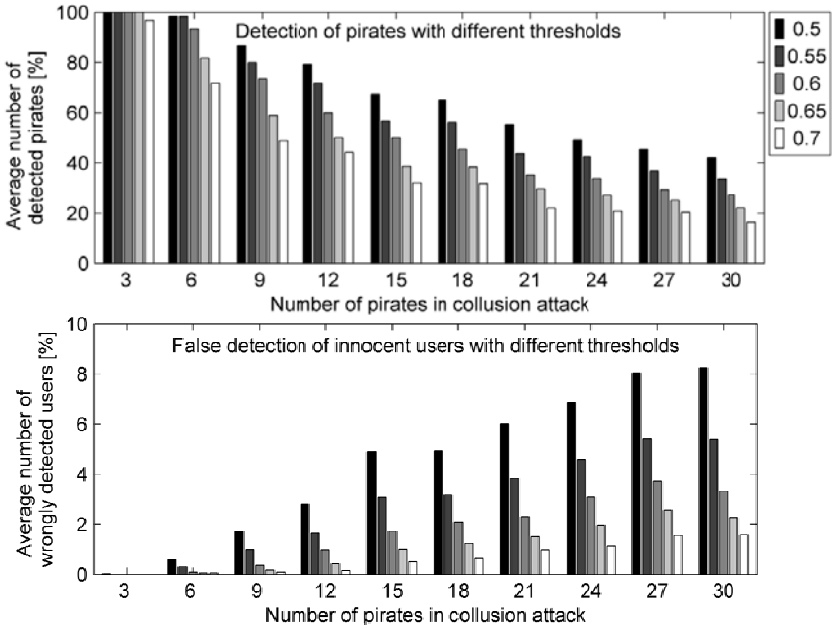

Fig. 5. Performance of the method in the case of sat1.bmp and set of fingerprints with values normally distributed [own study]

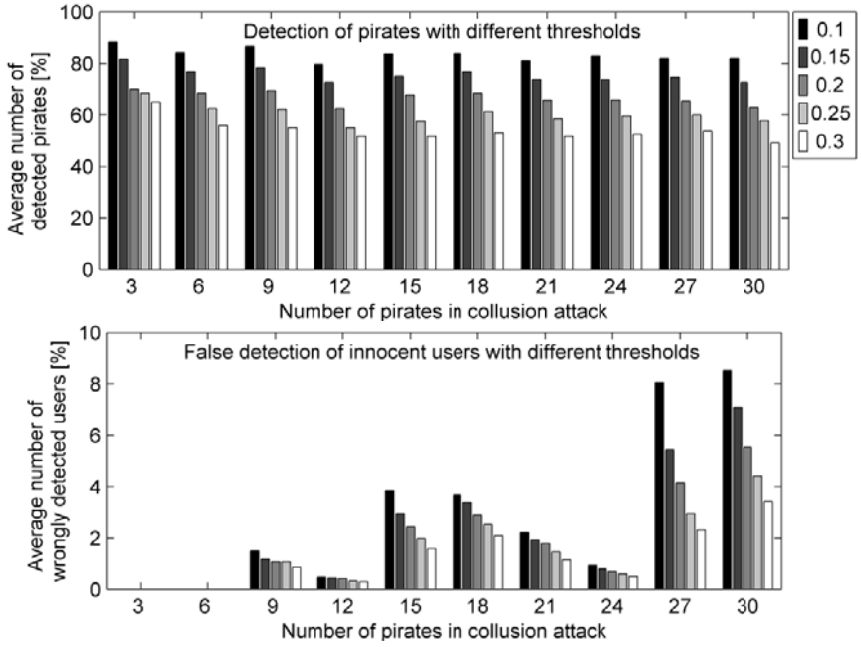

Fig. 6. Performance of the method in the case of sat1.bmp and set of orthogonal fingerprints [own study]

Although the orthogonal fingerprints undoubtedly give better results, it is hard to use them in practice because of their limited number. Usually the number of recipients is greater than the maximum number of possible orthogonal sequences of specific length.

CONCLUSIONS

The paper presents a modified fingerprinting method based on Hill cipher. Through studies have shown that it is possible to achieve high resistance to collusion attacks. Only static images had been used during tests but results can also be applied to the fingerprinting motion pictures because single video frames can be marked in the same way as used images. Future work will focus on embedding fingerprints in the frequency domain rather than pixels in order to achieve greater resistance to signal processing operations and collusion attacks.

This article should be considered as a discussion on securing the transmission of video images in VTS systems, which is very important in the era of increasingly crowded shipping lanes. The method proposed in the article could be very useful, because a network used to transmit secured data can be both wired and wireless.

REFERENCES

[1] Anderson R., Manifavas C., Chameleon — A new kind of stream cipher, Lecture Notes in Computer Science, Fast Software Encryption, E. Biham, ed. Heidelberg, Springer-Verlag, 1997, pp. 107–113.

[2] Barcz M., Review and analysis of fingerprinting methods for multicast distribution of video signals, Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, master thesis, 2009.

[3] He S., Wu M., Joint Coding and Embedding Techniques for Multimedia Fingerprinting, IEEE Transactions on Information Forensics and Security, 2006.

[4] Kundur D., Karthik K., Video fingerprinting and encryption principles for digital rights management, Proc. IEEE, 2004, Vol. 92, No. 6, pp. 918–932.

[5] Liu K. J. R., Trappe W., Wang Z. J., Wu M., Zhao H., Multimedia fingerprinting forensics for traitor tracing, EURASIP Book Series on Signal Processing and Communications, 2005, Vol. 4, Hindawi Publishing Corporation.

[6] Rykaczewski R., Hillcast — A method of joint decryption and fingerprinting for multicast distribution of multimedia data, Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics Annals, 2010, No. 8, series: Information Technology.

[7] Wu M., Trappe W., Wang Z. J., Liu K. J. R., Collusion-resistant fingerprinting for multimedia, IEEE Signal Processing Mag., 2004, Vol. 21, pp.15–27.

[8] Zhao H., Wu M., Wang Z. J., Liu K. J. R., Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting, IEEE Trans. Image Processing, 2005, Vol. 14, No. 5, pp. 646–661.

Received May 2012
Reviewed September 2012