electronics

MDPI

Article

CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia

Jinsu Kim [1,2], Namje Park [2,*], Geonwoo Kim [3] and Seunghun Jin [3]

1 Department of Convergence Information Security, Graduate School, Jeju National University, Jeju-si 63294, Korea; wlstn9498@daum.net
2 Department of Computer Education, Teachers College, Jeju National University, Jeju-si 63294, Korea
3 Information Security Research Division, Electronics and Telecommunications Research Institute, Daejeon 34129, Korea; kimgw@etri.re.kr (G.K.); jinsh@etri.re.kr (S.J.)
* Correspondence: namjepark@jejunu.ac.kr; Tel.: +82-64-754-4914

Received: 14 February 2019; Accepted: 18 March 2019; Published: 9 April 2019

Abstract: Intelligent video surveillance environments enable the gathering of various types of information about the object being recorded, through the analysis of real-time video data collected from CCTV systems and the automated processing that utilize the information. However, the surveillance environments face the risks of privacy exposure, which necessitates secure countermeasures. Video meta-data, in particular, contain various types of personal information that is analyzed based on big data and are thus fraught with high levels of confidentiality breaches. Despite such risks, it is not appropriate to implement encryption for video meta-data considering the efficiency issue. This paper proposes a character order preserving (COP)-transformation technique that allows the secure protection of video meta-data. The proposed technique has the merits of preventing the recovery of original meta information through meta transformation and allowing direct queries on the data transformed, increasing significantly both security and efficiency in the video meta-data processing.

Keywords: closed circuit television (CCTV); character order preserving; cloud system; privacy risk; security; video surveillance

1. Introduction

There has been a recent surge in the active introduction of intelligent video surveillance environments. Intelligent video surveillance technologies allow the collection and analysis of video information obtained from CCTV systems and the automated processing based on the information collected. These video surveillance technologies can be implemented in a range of subjects such as people, automobiles, buildings, and environment. When combined with cloud computing and big-data analysis techniques, the technologies offer the merit of enabling more significant situation recognition. Hence, they will likely allow the identification of risk factors with greater reliability through the analysis of the CCTV-fed live video footage and the subsequent implementation of appropriate countermeasures. The technologies, therefore, will serve as a core technology for intelligent security environments in the future [1].

Applications of intelligent surveillance technologies may include fire detection, prediction and monitoring for certain buildings or areas, environmental monitoring (air pollution, etc.), meteorological monitoring (typhoon, earthquake, tsunami, etc.), vehicle and traffic safety surveillance, and many more. Among them, crime prevention through behavior recognition-based risk detection is drawing attention as an important application. Currently, the City of New York (U.S.A) is operating the domain

awareness system (DAS), an intelligent crime prevention system, while Songdo International City (business district) in South Korea has put in place an International Business Machines Corporation's smart surveillance system called the smart surveillance solution (SSS). With the advancement of deep-learning technology, these intelligent video surveillance systems are likely to enable more reliable behavior recognition and risk-factor assessment through the analysis of accumulated data based on massive amounts of big data that are collected from CCTV camera recordings [2].

On the flip side, such technological advancement has various inherent risks. For instance, an intelligent video surveillance system under hacking attacks will lead to a serious social problem. Threats to the operation of video surveillance systems could result therefrom in various forms, such as malfunction or shutdown of the systems themselves, and exposure of video data collected from CCTV systems which could bring about personal information breaches [3–5].

In intelligent video surveillance systems (from now on, the "IVSS"), information regarding an individual's location, travel paths, and other details are collected from the CCTV system and stored in server or storage environments (cloud, etc.). The video information needs to be encrypted for safe storage. Even if the video information is breached due to hacking or other factors, the attacker can only obtain the encrypted data. Hence the confidentiality ensured. Encrypting video data for storage, however, is not a simple solution. Video information, being large-volume data, would require the process of decrypting the video data under analysis to their original condition, during which process the overhead issue can be a huge obstacle. To solve the problem, a policy may be put in place where all video data are analyzed and then encrypted before being stored. Still, there are additional problems of storing the analyzed meta-data. When video analysis meta-data are encrypted for storage, the same decryption overhead problem arises; when the meta-data are stored in plain-text files, hackers' obtainment of the meta-data alone will allow the leakage of considerable amounts of original CCTV video recordings, which is problematic as well. This paper, therefore, proposes a new meta-data security technique that is based on character order preserving (COP)-transformation to safeguard personal information contained in CCTV videos. The proposed COP-transformation method changes the information of plain-text meta-data to character-based information, thereby preventing the identification of original data. The new method is beneficial in that a keyword search is possible using the transformed meta-information alone because the string-order information about plain-texts is kept intact. Based on the proposed meta-information COP-transformation technique, both CCTV video data and meta-information can be protected against confidentiality breaches and can thus guarantee the security of privacy against exposure.

2. Related Studies

This chapter discusses the conventional techniques of protecting personal information contained in the video data. Furthermore, the need for video meta-data security is discussed as the topic is indicated herein as a security risk factor.

2.1. Conventional Methods of Video Privacy Protection

2.1.1. Video Privacy Masking Techniques

Privacy masking technologies refer to modifications that prevent facial information contained on video recordings from being recognized [6–8]. Examples of privacy masking include blurring, pixelation, and facial-region removal, all of which are fraught with the fundamental limitation that the original footage cannot be recovered fully when recovery is needed (see Figure 1).

Privacy masking technology has the merits of easy realization and privacy protection and is thus currently adopted by many CCTV security products. The merits notwithstanding, the future introduction of deep resolution, the big data-based video recovery technique, suggests the possibility of recovering blurred or pixelated facial regions close to the original footage using the disclosed video portions alone, and therefore there is no guarantee of security against privacy-breaches [9,10].

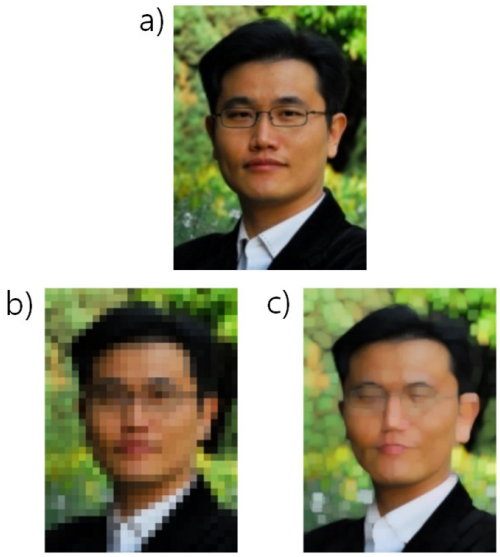

Figure 1. Example of privacy masking technology.

To complement the weakness of one-way privacy masking techniques, proposals have been made regarding partial encryption of the regions of interest (ROI) [9]. The partial ROI encryption method allows the encrypting of a particular region(s) on the video, such as a face. Encryption using this method prevents the recognition of facial information, just as the typical encryption algorithms do, but partial encryption allows the recovery of the original footage if the encryption key is used to decode the video. Still, the ROI-based method does not mention how to generate and protect meta-information regarding encrypted ROI information. Techniques for searching for a particular individual(s) on encrypted video storage and recovering him/her to the image on the original footage are virtually non-existent. If search meta-information is generated to that end at discretion, the subject of video can be fully disclosed in the meta-information concerned, which is problematic.

2.1.2. Cloud Encryption-Based Video Security

D.A. Rodríguez-Silva et al. proposed a cloud-based video surveillance environment [10] (see Figure 2). Since intelligent video surveillance environments characteristically handle large-volume data and are thus mandatorily required to accommodate expandability and availability, an Amazon S3-based expandable architecture is proposed. This architecture states that end-to-end encryption should be carried out using the Secure Sockets Layer (SSL) protocol to protect privacy. Regarding the encryption issue, it is mentioned that Amazon S3 takes care of security problems with the help of its own encryption applications. The proposed environment, however, has limitations in that it only covers the video information processing and storage method. In other words, the proposal states that the CCTV video data are subject to encryption in cloud environments but fails to mention how the meta-information is created for the video and how to be protected or how the encrypted data are searched. The proposed approach has limitations for implementation in big data-based intelligent video surveillance environments in the coming years [11–16].

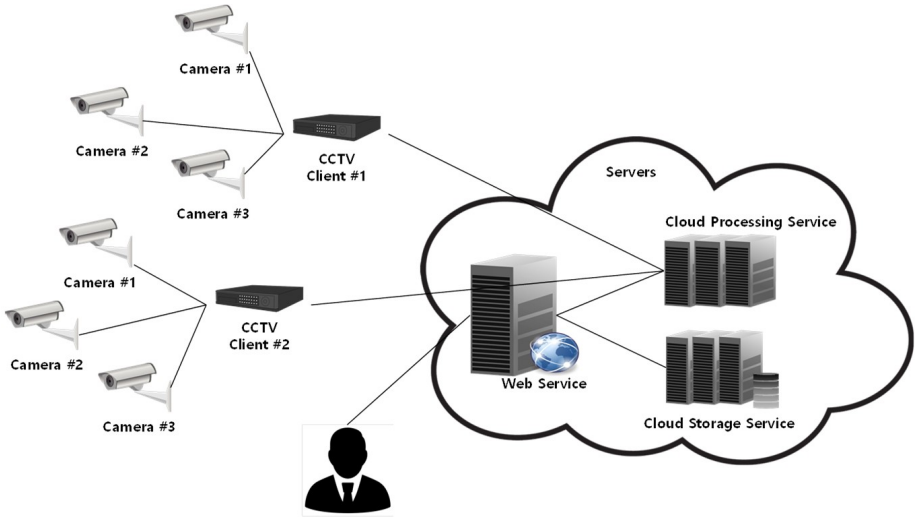

Figure 2. Video surveillance based on cloud storage. Reprinted with permission from reference [10]. Copyright 2012 IEEE.

2.2. Need for Protecting Video Meta-Data

2.2.1. Exposure of Personal Information in Video Meta-Data

Video surveillance environments in the future will not only recognize a particular individual by analyzing CCTV video data based on big-data technology but will recognize the individual's current behavior, analyze his/her behavioral patterns, and estimate the response as well. Hence, the scope of video meta-data is not just recognizing individual identities but it also includes the collection of many different types of information, such as a person's emotions, present condition, estimated behaviors, risk levels, and the recording thereof in the meta-data.

The video analysis meta-data could contain direct personal information. For instance, there could be ranges of real-time based analysis of a person's location tracking information, current behavior, and risk level judgment which is based on CCTV surveillance activities regarding certain individuals (suspects, etc.) for purposes of ensuring smart public order and safety environments. When the information is stored as meta-data, not only static personal information but dynamic personal information as well will be stored directly on a real-time basis, requiring more secure control and care. Even when hacking incidents take place aiming at meta-data, it is vitally necessary that the data security must be guaranteed [16,17].

When the attacker gains authority for accessing databases, he/she should be able to inquire about the video meta-information, in which process any set of video meta-data stored in plain-text files will be fully exposed to the hacker. In addition to the outside hackers' attacks, there have been a number of data leakage incidents committed by insiders. Given the risks, viewed from a privacy protection standpoint, storing meta-data as plain-text files will lead to serious personal information breaches and are considered extremely dangerous. In sum, security techniques appropriate for video meta-data should be introduced urgently.

2.2.2. Incompatibility Between Video Privacy Protection and Efficiency

When video metadata are stored in the database, not as plaintext files, but as cipher-text ones, there comes the problem that makes range search/queries extremely difficult.

For instance, a search for an individual who approaches a location within a certain range on video will prevent the user from executing a range search/query as long as the information is encrypted. The search failure is caused by string order in the encrypted data which is different from that of plain-text files. Launching a range search based on the results of encrypted data will lead to a set of data completely different from what was desired [18–21].

As a solution to the problem, the order-preserving encryption (OPE) approach has been proposed [15–17]. Using OPE, however, can weaken the security now that the encrypted values will have the same string order as the plain-text files. Moreover, the OPE technique has the disadvantage that the original data sets must be created in numerical data. There is a difference between the way characters and numbers are sorted. For example, numerical data in the database regard 20 as the smaller value than 100, whereas character strings consider 20 the larger value. Video meta-data exist in various forms but are mostly treated as numerical data or character strings. The existing OPE algorithms can only process numerical data. Since the algorithms cannot handle character strings, they are not fit for executing video meta-data security measures. It is not easy to ensure both confidentiality and data-search efficiency because a successful data search would require even the smallest amount of information about the original data, and as a result, maintaining confidentiality becomes practically infeasible. As such, privacy protection and efficient video surveillance are challenges that are difficult to resolve simultaneously. However, as video recognition technology advances steadily in the future, and as more meticulously analyzed video information based on big data applications is expected to be recorded in detail on meta-data servers, the issue of privacy in video surveillance environments simply must be resolved. The South Korean legal system has already stipulated the need for firm security regarding CCTV video data. Stated under Article 25-6 (Limitation to Installation and Operation of Visual Data Processing Devices) of the Personal Information Protection Act, the "VDPD operator" must take measures necessary to ensure data security so the personal information is protected against loss, theft, leakage, forgery, alteration, or damage. As it stands, due considerations are necessary [22–26].

3. Proposed Method

This chapter investigates the video security surveillance environment (model) proposed by this paper and suggests COP-transformation algorithms and a technique to securely protect CCTV video data in intelligent video surveillance environments using the algorithms.

3.1. Overview of the Proposed Technique

CCTV Video Security Surveillance Environment Model

Figure 3 illustrates the proposed video security surveillance environment. In this model, the CCTV system records the video on a real-time basis and stores the image data in cloud storage. The cloud storage in the surveillance system is where video recordings are encrypted and kept. Meanwhile, the CCTV video footage is subjected to the generation of big data-based real-time meta-information which is stored using the proposed COP-transformation algorithms. In the process, under no circumstances are the data stored in a plain-text format.

An authorized CCTV surveillance staff member collects and verifies the video data fed from the CCTV surveillance system. In such an environment, the direct query can be launched for the video footage based on the COP-transformation meta-data, and the authorized staffer may search the footage based on query results and bring up the images. For instance, it is possible to launch an image search using the query "Are there any images that put John in Area A at around 10 p.m.?" CCTV meta-information is a type of personal information, and as such, it can have a massive security flaw when stored as plain-text files. The information, therefore, should be stored as transformed meta-data files using the COP-transformation model proposed herein.

The proposed model leaves no trace of the plain-text meta-information and the CCTV video data in a plain-text format in the CCTV surveillance environment; hence the privacy of CCTV video data is ensured. In other words, even when a hacker attempts to infiltrate into the CCTV surveillance environment (network), for the purposes of stealing video information and meta-data, and has succeeded in obtaining these data, he/she cannot recover the plain-text files. This characteristic also has the merit of preventing insider attacks launched by internal staffs such as CCTV surveillance system related operators. A normal way to bring up the video data of interest would be through a

COP-transformation query performed in the defined manner and by an authorized surveillance staff member. No unauthorized individuals can locate or crack the original data.

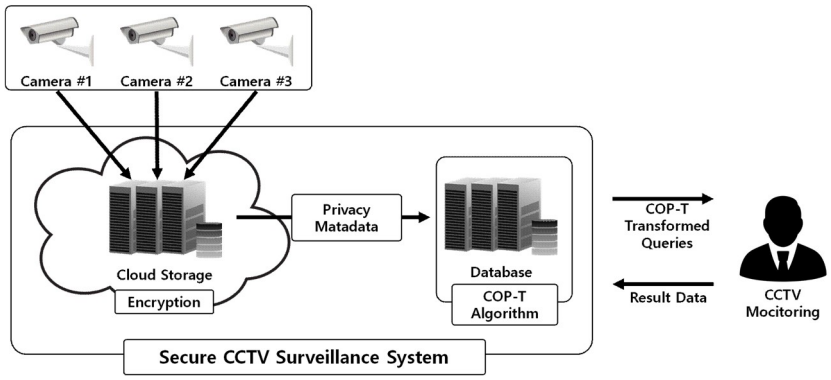

Figure 3. Overview of the proposed scheme.

3.2. Detailed Procedure

3.2.1. Abbreviation

The abbreviations (notation) used to describe the proposed technique (see Table 1).

Table 1. Notation.

Abbreviation	Content
D, R_{-1}	Pre-shared Initial Seed
C_i	i-th Character of C
P_i	i-th Random Scale Value
R_i	i-th Pseudorandom Number
DIG $(\cdot)$	Result of Digitalization
CHR $(\cdot)$	Result of Characterization
$PRNG$ $(\cdot)^s$	Pseudorandom Number Generation
T_i	i-th COP-Transformation Value
x	The Last Element of Domain
n	Source String Length

3.2.2. COP-Transformation Algorithm Design

(1) Overview of COP-Transformation Model

The COP-transformation technique replaces the strings in the original files with the transformed characters via a conversion function. The conversion is carried out in single-character units (character by character) that are part of the character strings in whole. The process has the following characteristic. The domain of particular strings and that of the transformed strings have their respective sorting order; however, the sorting order in the transformed strings domain is not necessarily the same as that in the plain-text files and is instead determined by the operation shown below:

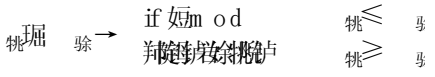

Figure 4 presents the COP-transformation method in a simple diagram, whereas Figure 5 shows the actual COP-transformation algorithms.

The COP-transformation technique consists of three phases: (1) digitalization (turning single characters into numerical values); (2) random scale (computing random evaluations based on the character strings domain using pseudo-random numbers); and (3) scale transformation (converting the random evaluations into new evaluations, and the scale conversions into characters).

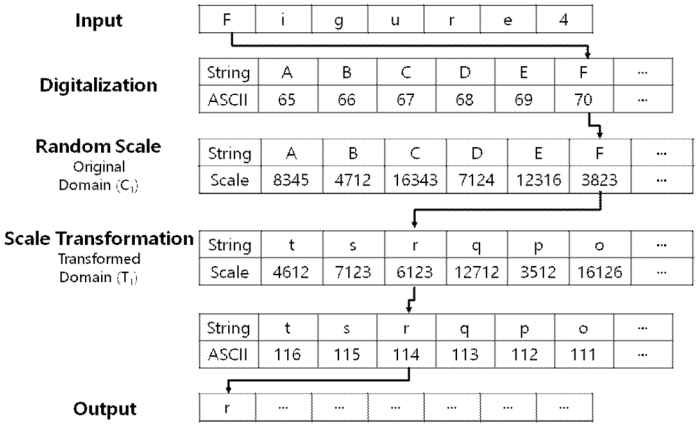

Figure 4. The concept of COP-transformation.

Algorithm: COP-Transformation

i=0
While i≤n do
  A_i = DIG(C_i)
  $s=R_{i-1} + D$
  $R_i = PRNG(i)^s$
  ›桃 森 躬 躬 ⩔ ♡ 躬防
  j=0, u=0
  while u≤P_i do
    $M_j = PRNG(j)^{s+1}$
    u = M_j + u
    j=j+1
  end
  if (R_i mod 2) = 0 then
    T_i = CHR(j)
  else
    T_i = CHR(DIG(x) - j)
  end if
  I = i+1
end

Figure 5. COP-transformation algorithm.

(2) Digitalization Phase

In the COP-transformation model, substitution takes place in a series of single-character units utilizing the strings in the original file. First, a single character is converted into a number according to the pre-defined mapping table. The simplest example would be a conversion into ASCII codes, where the table characteristically includes everything—letters, numbers, and character entities. Character sets, i.e., the outputs of the characters converted by input-specific computation, apply

to the entirety of the mapping table as defined. Hence, when the mapping table adopts ASCII codes, the COP-transformation results will include character entities even if the original file is composed only of ordinary numbers and letters. In other words, the mapping table used in the digitalization phase will create no problems with the operation when the conventional ASCII codes are implemented; however, the outputs (results) may include character entities (see Figure 6).

Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex
(sp)	32	0040	0x20	@	64	0100	0x40	`	96	0140	0x60
!	33	0041	0x21	A	65	0101	0x41	a	97	0141	0x61
"	34	0042	0x22	B	66	0102	0x42	b	98	0142	0x62
#	35	0043	0x23	C	67	0103	0x43	c	99	0143	0x63
$	36	0044	0x24	D	68	0104	0x44	d	100	0144	0x64
%	37	0045	0x25	E	69	0105	0x45	e	101	0145	0x65

Figure 6. ASCII-based mapping table.

(3) Random Scale Phase

This phase involves the measuring of random scale values that correspond to the numerical information generated in the digitalization phase. To that end, seeds of the pseudo-random numbers should first be determined. The initial values of the numbers are determined to be D, i.e., the previously shared value. The D value is what is needed in the process of subjecting the original data to COP-transformation and will invariably be needed during converted data search later on. Without knowing the D value, normal search sessions cannot take place. Following the initial single-letter conversions, a value that is the sum of Ri-1 and D will be used as a seed necessary for Ri operations.

Pi (random scale number) is determined by totaling the pseudo-random numbers PRNG(k)s. The random scale number Pi which corresponds to the i-th block in the original strings can be obtained from the formula below:

(4) Scale Transformation Phase

In this phase, new mapping numbers are computed based on the Pi numbers that were generated in the preceding random scale phase. For this phase, the seed is defined as the number that is the sum of "s" (previously computed seed) and 1. Once the seed is defined, the number generation is repeated until the total of the pseudo-random numbers generated by using the seeds reaches the random scale output Pi while counting the number of repetitions "j." Figure 5 shows the process of generating "u" based on PRNG(j)s+1.

The number of repetitions "j" so computed will be the input number for the mapping table when the final outputs (characters) are obtained. As previously mentioned, the seed implemented during scale transformation is different from the seed in the random scale phase. Hence the initial numerical outputs do not match the numbers generated in the scale transformation phase. Applying these output values conversely to the mapping table used in the digitalization phase and substituting with particular letters will lead to the final conversion outputs. The mentioned steps should be repeated until reaching the end of the strings to obtain the COP-transformation strings corresponding to the entirety of the strings.

3.2.3. CCTV Video Data Mapping Structure

CCTV videos are encrypted and then kept in storage. As encryption algorithms, symmetric encryption algorithms such as advanced encryption standard (AES) can be used. Once encrypted,

video files are assigned a video ID, respectively. Each video file splits into several files, with an individual chunk ID given to each of them. Characteristically large-volume, a CCTV video file must have in its directory multiple separate chunks. For instance, when searching the list of CCTV video files that feature, for example, "John", the search efficiency would be significantly reduced if all of the files created on a certain date are decoded. Instead, securing the list of detailed chunks showing "John" in each video file concerned will only necessitate the ensuing decryption of the files in question, hence hugely advantageous in terms of video decoding efficiency. This paper, therefore, proposes an architecture where video data are divided into smaller chunks (files) and then encrypted individually before being stored. In such implementation, the video IDs and chunk IDs that match the tag search information are secured, and only those portions of the files that correspond to the chunk IDs are subjected to encryption. Hence, performance efficiency is achieved. In the same process, if encryption covers only the CCTV video files and the meta-data are stored in a plain-text format, privacy protection can be a huge challenge because the meta-data alone can disclose in detail the content of video files. This paper, therefore, proposes CCTV videos be encrypted and at the same time video meta-data be stored as COP-transformation outputs. Since the plain-text files are not to be stored anywhere in the meta-database, or the storage, the target individual's personal information as contained on the recordings can be securely protected. Figure 7 illustrates the mapping structure between video meta-data and actual video footage.

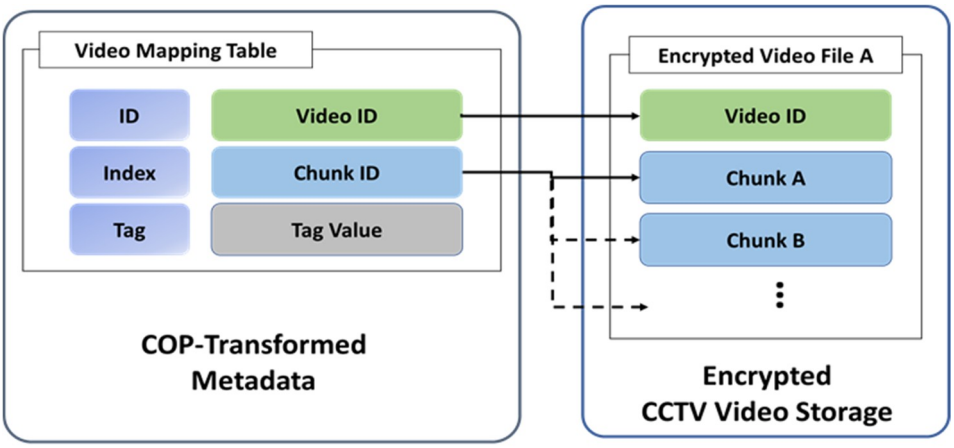

Figure 7. Video data mapping structure.

3.2.4. COP-Transformation Meta Query Technique

The meta outputs converted via the COP-transformation technique have the merit of allowing direct query on meta-data even when they exist as the converted meta inputs and not the plain-text files in the database. COP-transformation data characteristically enables, not only direct right-hand truncation and range searching, but also aggregation for statistical applications. Another merit is that the database index architectures can be used as they are. Encrypted databases cannot utilize indexes for right truncation, range searching, etc. other than the match query, causing a significant drop in database efficiency. On the contrary, the COP-transformation method allows the use of indexes during the database query, with the resulting efficiency showing no practical difference when compared with that of the plain-text query. A significant advantage of the method is that it can avoid the disclosure of plain-text data and at the same time improve the performance of the database query process.

Figure 8 shows how a typical SQL (structured query language) range query is changed into a COP-transformation query. Using the COP conversion numbers, the order in plain-text files is stored at random as either forwarding or reverse, which is determined based on "u," the output extracted in the scale transformation phase. In other words, the process characteristically changes the size of outputs during range search, depending on the result of Ri mod operations. The COP-transformation data are characterized by the application of random assignment of sorting order in plain-text files, which is

either in forwarding or reverse order for each cipher of the strings. Hence, the normal query on the data is feasible only when the Ri number is known. Of note, changing the parameters will allow query (range search, aggregation, etc.) to take place even when the sorting in plain-text data is in reverse order. For instance, if users intend to bring up the upper 30th percentile of data, they will obtain the same outputs in a reverse order scenario by taking the lower 30th percentile of the data. Therefore, the proposed COP-transformation implementation is unique in that it can still execute range search and aggregation without maintaining the whole sorting in a forwarding order.

Original Query:

select video_id, video_idx

from metadata

where tag > C_a *and tag* < C_z

Transformed Query:

select video_id, video_idx

from metadata

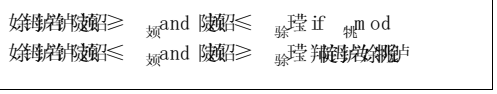

Figure 8. COP-Transformation of SQL Query.

In cases where hackers, or other types of predators, without the proper authority launch an attack, they cannot recreate the transformation query because they are not aware of the previously shared values D, R-1, and s (seed of pseudo-random numbers) and thus unable to generate Ta and Tz numbers. Even if they knew the Ca and Cz numbers, they are still unable to access the information.

4. Implementation

4.1. Performance Evaluation

This section of the paper examines the results of performance evaluation obtained by the proposed method. The performance measuring environment for the COP-transformation algorithms is as follows. The algorithms were realized in C++ language and the database using the SQLite tool. The CPU adopted was for i7-4790K@4.0GHZ (Windows 10) environments and the memory capacity used was 6GB of RAM. Figure 9 presents the results of the evaluation. The highest level of performance was found when the database query was executed in a plain-text format, whereas no substantial difference in performance was found between the OPE mechanisms and the proposed one in real terms. The reason behind the results is that all three approaches had utilized database indexes, thereby bringing up the data at high speed. Furthermore, only the encryption implementation time was added to the indexed database processing time. Of note, the implementation of AES encryption does not accommodate database indexing, which led to the confirmation that extremely large amounts of overheads were required for the database query.

Executing database query in a plain-text format and the proposed COP-transformation mechanism has shown only a slight difference in the query processing speed. The same characteristic was observed in the conventional OPE applications; nonetheless, the traditional systems are inherently susceptible to security breaches because of their sorting order which is the same as that of plain-text files, which consequently allows analysis-attacks on the data. The proposed COP-transformation technique shows a comparable level of performance when compared to the plain-text format and OPE applications. The proposed mechanism offers the merit of stronger security thanks to the random assignment

of order information (reverse or forwarding) which is different from that of plain-text files. Typical encryption algorithms such as AES cannot utilize database indexing solutions and thus cause extremely large overheads. The finding shows that the proposed method offers a higher efficiency compared with the conventional encryption approaches.

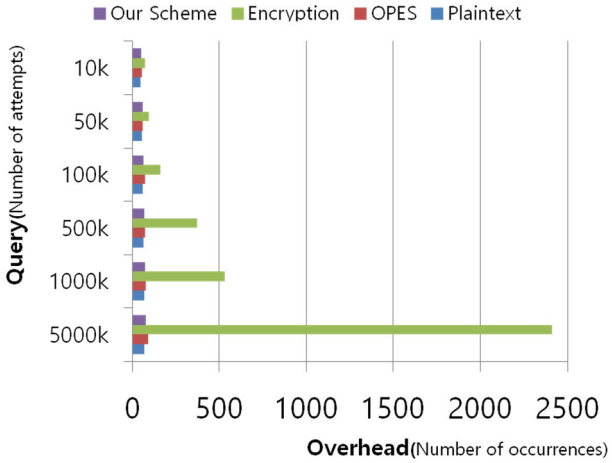

Figure 9. The time overhead in the range query.

4.2. Video Meta Query Handling

Figure 10 (image on the left) lists the entirety of the data, while the image on the right shows the range query that was reconstructed from the COP-transformation process. The COP-transformation query outputs show that they deliver the same result as do the query results generated in plain-text-based database environments. Furthermore, the proposed mechanism has the same execution scheme (explain query plan) as the plain-text environments, meaning it can perform a query with efficiency because indexing can be put to use even in the converted state in the same way as the plain-text environments.

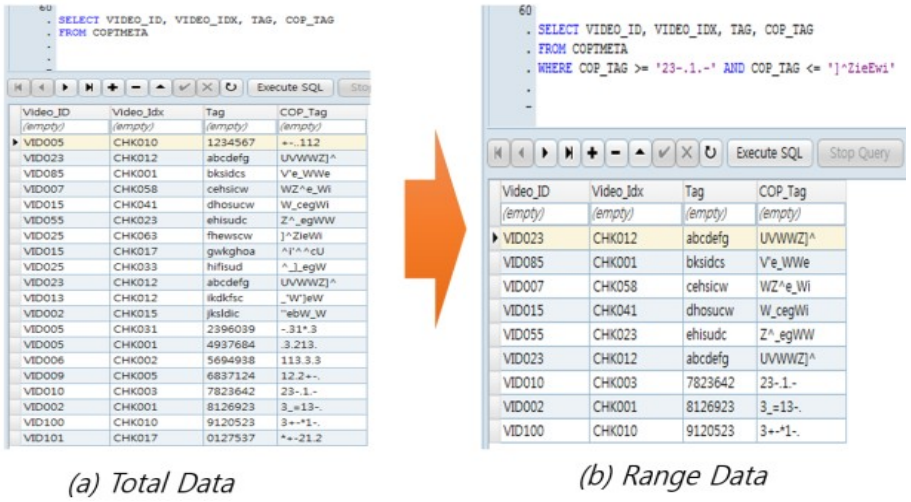

Figure 10. COP-transformation of SQL query.

5. Analysis

5.1. Security Analysis

5.1.1. Exposure of Video Data to External Applications

Video data consist of the meta-database where meta-information is stored and the video storage where actual CCTV video recordings are kept. Given the characteristic, CCTV video data are considered personal information because the visual data on the recordings alone can allow first-hand verification of personal information as recorded, such as the person's location and movement. The analysis information is recorded in the video meta-data, and the video CCTV data and video meta-data themselves constitute risks of privacy breaches. The most secure countermeasure would be encrypting the data. The technique proposed herein implements encryption to all CCTV video data that are stored in actual storage solutions. Even when attackers breach the video data in the storage, data security can still be ensured. Of note, the video meta-data exist in the form of converted data that utilize the proposed COP-transformation; hence, attackers are unable to reconstruct the COP transformation numbers unless aware of D (initial confidential value as shared) and the initial seed numbers necessary for generating pseudo-random numbers. In other words, nowhere in the meta-information or CCTV video data exists the personal information stored directly in a plain-text format. Even if the entirety of the video data is unavoidably disclosed to external applications, data security remains intact.

5.1.2. Disclosure of Meta Query Process

Simply by obtaining the SQL query used for meta-information searching during search-minded meta-information query sessions and the query execution results, the content of CCTV video recordings can be guessed. Contrastingly, the proposed method does not disclose plain-text-based meta-data on the SQL server during the video meta query. Moreover, the entirety of meta-information outputs in the database is converted via COP-transformation; as such, the outputs searched through SQL query, too, are returned as converted numbers. In sum, even if attackers got to obtain all of the video meta queries and returned data, data security remains intact because hackers cannot recover the original plain-text data from the converted values.

5.1.3. Insider Attacks

CCTV video recordings are commonly stored in cloud storage due to the sheer size of the data. Particularly in cloud environments, it is necessary to guard against attacks from insiders (cloud system operators, etc.). Such insiders can gain access to the database and storage at any time. The proposed technique allows the sharing of D (initial shared value) only amongst authorized individuals. Furthermore, the databases including meta-information are already converted through COP-transformation, and the storage CCTV video data are encrypted for all of the files. It would be necessary to separate the implementation of access control, i.e., file and data access authority from the administrator's end (insiders, etc.) vs. plain-text-data verification authority on the part of the actual video surveillance staff. In other words, D (initial shared value) and R-1 must be shared only amongst the personnel having the actual viewing authority. Which means the cloud storage administrator/manager may access the encrypted data but may not recover the plain-text information from the database or storage unless otherwise authorized to view the information.

5.2. Efficiency Analysis

5.2.1. Video Data Decoding Performance Considerations

When the entire CCTV video data are encrypted, obtaining the video files fitting certain conditions would require the decoding of the whole file(s) in question, despite any meta-query that is executed. This process can act as a factor that reduces the data search speed significantly, and as such, is inefficient.

The proposed method characteristically divides the data into multiple chunks during encryption. A video meta-data query can therefore be executed based on the chunk ID that is assigned to the part of the video file that corresponds to the segment of the video footage. The proposed mechanism carries out decryption by avoiding the decoding of the whole CCTV video data and instead obtains only the partial video data that satisfies the chunk-based search parameters. Efficiency, therefore, is ensured by the new method in terms of the data decoding performance.

5.2.2. Efficiency in the Query Design

When creating query statements for meta-information search, data utilizing the COP-transformation technique will enjoy query-processing efficiency on a par with those using plaintext files. In other words, COP-transformation implemented databases can execute not only the match query, right-hand truncation, and range query but also the queries utilizing joins for multiple tables. Moreover, they can create simple query statements during the statistical analysis of the meta-information. For instance, the proposed technique is beneficial in that it allows for the implementation of aggregations that are necessary for statistical processing under certain conditions (e.g., min, max, count, avg), directly to the meta-data that were subjected to COP-transformation. Such merit cannot be realized when the database exists in a simple encrypted state. If the database is to be encrypted using a typical method, it would be extremely difficult in real terms to construct query statements except for match query statements. For example, when range query is needed, creating direct SQL range-query statements will be infeasible unless the entirety of the data has been encrypted and stored separately because encrypted databases have a different sorting order than that adopted by plain-text outputs. The method proposed herein allows not only the implementation of range query using COP-transformation applied meta-data themselves but also the use of database index information as it is, thereby increasing efficiency in processing speed. Table 2 indicates whether or not query processing is feasible under the three meta-information conditions: (1) in plain-text files; (2) in an encrypted state; and (3) as converted data via COP-transformation. Plain-text files allow match query, range query, and aggregation, whereas encrypted meta-data render infeasible the creation of range query and aggregation statements other than match query ones. The proposed mechanism accommodates match query, range search, and aggregation just as plain-text data would allow; furthermore, it allows the use of database indexes as they are and thus ensures processing efficiency.

Table 2. Efficiency comparison.

Query Type	Plaintext	Encryption	The Proposed Method
Equation query	○	○	○
Range query	○	×	○
Aggregation query	○	×	○

6. Conclusions

With the advancement of artificial intelligence (AI) technology in the coming years, techniques and markets for CCTV-based smart video analysis applications are expected to develop enormously. CCTV video recordings, however, contain personal information in plain view; as such, countermeasures for privacy protection are essential. Traditional video data protection approaches rely on masking or simple encryption. They do not offer efficient and secure CCTV video searching algorithms that are based on video meta-data. In real-world applications, encrypting meta-data will prevent searching other than match query, and thus meta-data are typically stored in a plain-text format. The meta-data contains large amounts of information about video recordings, which will likely lead to the disclosure of even larger amounts of personal information, as found in video meta-data, while the big data-based video analysis technology is further advancing in the future.

Based on this rationale, this research paper proposed a COP-transformation technique. The method has the merit of increasing video meta-data efficiency significantly by allowing database query to take place in the same way as that adopted for plain-text files, without leaving the plain-text files exposed. To describe the proposed mechanism, first, chapter 2 investigated the conventional video privacy protection techniques and the need for video meta-data protection. In chapter 3, details were provided regarding the proposed COP-transformation algorithms and the way of generating query sessions to search video meta-information. The descriptions were followed by chapter 4 where the proposed technique was implemented for a real-world environment application, and its performance was measured. Chapter 5 analyzed the proposed algorithms from the standpoint of security and efficiency.

With prospects of more meticulous, big data-based video analysis solutions on the horizon, increasingly larger amounts of information will find their way into video meta-data in the coming years. Such prospects can be directly related to the invasion of recordees' privacy; as such, secure countermeasures must proceed. With the advent of the fourth industrial revolution era approaching, more research will be needed to address security techniques for intelligent video surveillance environments. Such techniques will likely position themselves as a mandatory privacy protection mechanism to ensure a safer, more secure society in the future.

Author Contributions: Conceptualization, N.P.; Data curation, G.K.; Methodology, S.J.; Project administration, N.P.; Writing—original draft, J.K.

Funding: This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (2017-0-00207, Development of Cloud-based Intelligent Video Security Incubating Platform) and this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A3A03918513).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Park, N.; Kim, M. Implementation of load management application system using smart grid privacy policy in energy management service environment. *Clust. Comput.* **2014**, *17*, 653–664. [CrossRef]
2. Lee, D.; Park, N. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. *J. Supercomput.* **2017**, *73*, 1119. [CrossRef]
3. Park, N.; Hu, H.; Jin, Q. Security and Privacy Mechanisms for Sensor Middleware and Application in the Internet of Things (IoT). *Int. J. Distrib. Sens. Netw.* **2016**. [CrossRef]
4. Dufaux, F.; Ebrahimi, T. Scrambling for Privacy Protection in Video Surveillance Systems. *IEEE Trans. Circuits Syst. Video Technol.* **2008**, *18*, 1168–1174. [CrossRef]
5. Agrawal, P.; Narayanan, P.J. Person De-identification in Videos. *IEEE Trans. Circuits Syst. Video Technol.* **2011**, *21*, 299–310. [CrossRef]
6. Dufaux, F.; Ebrahimi, T. A Framework for the Validation of Privacy Protection Solutions in Video Surveillance. In Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), Singapore, 19–23 July 2010; pp. 66–71.
7. Newton, E.M.; Sweeney, L.; Malin, B. Preserving Privacy by De-identifyuing Face Images. *IEEE Trans. Knowl. Data Eng.* **2005**, *17*, 232–243. [CrossRef]
8. Sang, C.G.; Tae, S.Y. Personal Video Privacy Issue to Increasing CCTV Installation. *J. Comput. Sci. Eng.* **2009**, *27*, 25–33.
9. Peng, F.; Zhu, X.; Long, M. A ROI Privacy Protection Scheme for H.264 Video Based on FMO and Chaos. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1688–1699.
10. Rodríguez-Silva, D.A.; Adkinson-Orellana, L.; González-Castaño, F.J.; Armiño-Franco, I. Video surveillance based on cloud storage. In Proceedings of the 2012 IEEE Fifth International Conference on Cloud Computing, Honolulu, HI, USA, 24–29 June 2012; pp. 991–992.
11. Lee, D.; Park, N. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *Pers. Ubiquitous Comput.* **2017**. [CrossRef]

12. Lee, D.; Park, N. A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud. *J. Korea Inst. Inf. Secur. Cryptol.* **2016**, *26*, 929–940. [CrossRef]
13. Park, N. Implementation of inter-VTS data exchange format protocol based on mobile platform for next-generation vessel traffic service system. *Information* **2014**, *17*, 4847–4856.
14. Park, N.; Kang, N. Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. *Sensors* **2015**, *16*, 1–16. [CrossRef]
15. Agrawal, R.; Kiernan, J.; Srikant, R.; Xu, Y. Order preserving encryption for numeric data. In Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, Paris, France, 13–18 June 2004.
16. Kim, D.; Lee, H. Personal Information De-Idenification Trends based on Big Data. *Rev. Korean Soc. Internet Inf.* **2015**, *16*, 15–22.
17. Lee, D.; Park, N. A Study on Metering Data De-identification Method for Smart Grid Privacy Protection. *Korea Inst. Inf. Secur. Cryptol.* **2016**, *26*, 1593–1603. [CrossRef]
18. Bruen, A.A.; Forcinito, M.A. *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2005.
19. Lee, D.; Park, N. A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance. *J. Korea Inst. Inf. Secur. Cryptol.* **2018**, *28*, 417–428.
20. Park, N. Design and implementation of mobile VTS middleware for efficient IVEF service. *J. KICS* **2014**, *39C*, 466–475. [CrossRef]
21. Park, N.; Kwak, J.; Kim, S.; Won, D.; Kim, H. WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. *Adv. Web Netw. Technol. Appl. LNCS* **2006**, *3842*, 741–748.
22. Park, N.; Bang, H.-C. *Mobile Middleware Platform for Secure Vessel Traffic System in IoT Service Environment. Security and Communication Networks*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2016; Volume 9, pp. 500–512.
23. Lee, D.; Park, N.; Kim, G.; Jin, S. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. *Peer-to-Peer Netw. Appl.* **2018**, 1–10. [CrossRef]
24. Lee, D.; Park, N. ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment. *J. Ijet* **2018**, *7*, 151–154.
25. Park, N. Information Exchange between VTSCs for Secure Next-generation Vessel Traffic System. *Int. Inf. Inst. (Tokyo). Inf.* **2017**, *20*, 1309–1316.
26. Lee, D.; Park, N. Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management. *Trans. Korean Inst. Electr. Eng.* **2018**, *66*, 1879–1888.