The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images: A comparison study

Polawat Witoolkollachit

Department of Information Technology, King Mongkut's University of Technology North Bangkok, Thailand

Abstract

Symmetric encryption technology is widely used in internet security systems. To keep images secure, image encryption technique is a specific security process. The encryption technique should be strong enough to prevent breaking the algorithm. The integrity checking of the encrypted image file can detect whether any critical system files have been changed, thus enabling the system administrator to look for unauthorized alterations of the system. Hash function is the desired function for hash value comparisons. This study focused on the comparison of the avalanche effect on the various hash values of images before and after various encryption techniques and which of the combined encryption techniques and then hash functions show the maximum avalanche effect. According to this study, the combination of Blowfish, AES-256 and DES against SHA-1, HMAC-SHA256, and CMAC-SHA256, showed no statistical significance in terms of the averages of the avalanche effect but the RC4 and 3DES were statistically significant. However, the RC4 encrypted image group had a lesser average avalanche effect than 3DES. The 3DES encrypted image group with CMAC-SHA256 showed the best avalanche effect with statistical significance among the SHA-1 and HMAC-SHA246 groups.

Keywords: avalanche effect, encrypted raw images, non-encrypted images.

Received 20 December 2015; Accepted 25 March 2016

Introduction

Symmetric encryption technology is widely used in internet security systems.[1] It utilizes a confusion and diffusion technique to encrypt the subject. The time of encryption is the most sensitive variable for encryption security techniques. Most people expect immediate results from encryption techniques. Image encryption is a common security process. The encryption technique should be strong enough to prevent breaking the algorithm.[2,3] The integrity checking of the encrypted image file can detect whether any critical system files have been changed, thus enabling the system administrator to look for unauthorized alteration of the system. Hash function is the desired function by hash value comparison.[4,5]

Avalanche effect is one of the desirable properties of cryptographic algorithms, typically blocking ciphers and cryptographic hash functions.[6] This phenomenon is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes

Correspondence: Polawat Witoolkollachit, Department of Information Technology, King Mongkut's University of Technology North Bangkok, Thailand (Tel.: +66-2555-2708; E-mail address: Polawat.w@gmail.com).

significantly. If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a cryptanalyst can make predictions about the encryption algorithm of the input by seeing the cypher texts. This may be sufficient for guessing the difficulty to break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device.

The wide use of high resolution images in medical care such as X-ray images, photos of wound characteristics are common in the present medical practice. The hospitals must keep all image files secret by privacy law. The integrity checking of the encrypted images by hash values is currently the most favorable technique.[7] Therefore, the collision resistance property must be of concern.

This study observed two groups of ten images. The original images are the same in both groups. The first group was unencrypted RAW images which received hash function application. The hash values were recorded. The hash values from this group were used as the control group. The second was five different symmetric encryption algorithms namely; AES-256, DES, 3DES, RC4 and Blowfish against 19 raw images. Then the hash function was applied to all images and all hash values were recorded. The purpose of this study was to determine differences in the avalanche effect of various hash functions on the encrypted image groups compared to the avalanche effect of hash function of the non-encrypted image group and which pair had the greatest avalanche effect. This study also used statistics to test the differences of variance of the mean avalanche effect between all observed groups.

Related Work

RC4 has a utilization in both encryption and unscrambling while the information stream experiences XOR together with a progression of created keys.[8] It takes in keys of irregular lengths and this is known as a maker of pseudo subjective numbers. The yield is then XORed together with the flood of information to create recently encoded information. Consequently, a specific RC4 key ought to never be used again when scrambling two other information streams.

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier[9] and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

AES is a symmetric key block cipher. It uses a fixed 128-bit block cipher and three key lengths supported by AES as this was an NIST design requirement.[10] The number of internal rounds of the cipher is a function of the key length according to the Hash based message authentication code (HMAC) and has been the mandatory-to implement MAC for IPSEC. HMAC based on secure hash algorithm (HMAC-SHA-1) has been recommended for message authentication in several network security protocols. The key reasons behind this were the free availability, flexibility of changing the hash function and reasonable speed, among others. The MAC based on the block ciphers such as CBC-MAC-DES was generally considered slow due to the complexity of the encryption process.

DES is the archetypal block cipher,[11] an algorithm that takes a fixed-length string of plain text bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES (3DES)[12] provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

A cryptographic hash is a kind of 'signature' for a text or a data file. These functions are mathematical operations run on digital data. By comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A key aspect of cryptographic hash functions is their collision resistance: noone should be able to find two different input values that result in the same hash output.[13] SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. See below for the source code.[14] SHA-256 is novel hash function computed with 32-bit words. It uses different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds.

Analysis of variance (ANOVA)[15] is the most commonly used technique for comparing the means of groups of measurement data. There are many different experimental designs that can be analyzed with different kinds of ANOVA. In a one-way ANOVA (also known as a one-factor, single-factor, or single-classification ANOVA), with one measurement variable and one nominal variable which makes multiple observations of the measurement variable for each value of the nominal variable.

Material and Methods

The 19 raw images were randomly selected in this study. **(Figure 1)** A sample size calculator was used to determine sample size needed with a fixed parameter (95% confidence level, 5% confidence interval, population =20). The raw files were taken from FUJINON X-T10. This camera uses a 16 million mega pixels photo sensor and processes image internally by 14 bits color depth. All images are 4896x3264 in dimensions. The size of image is between 31 and 33 MB. The notebook Intel core i7 3.06 MHz CPU, Ram 8 GB, 256 GB SSD, VMware workstation 12.0 and windows 10 environment was used for this study. The CentOS 7.0 64 bit guest OS with 2 GB Ram was updated to the latest version. During the experiment, the use of external power supply prevents CPU changing to low power environment automatically with the maximum power scheme in windows host machine.

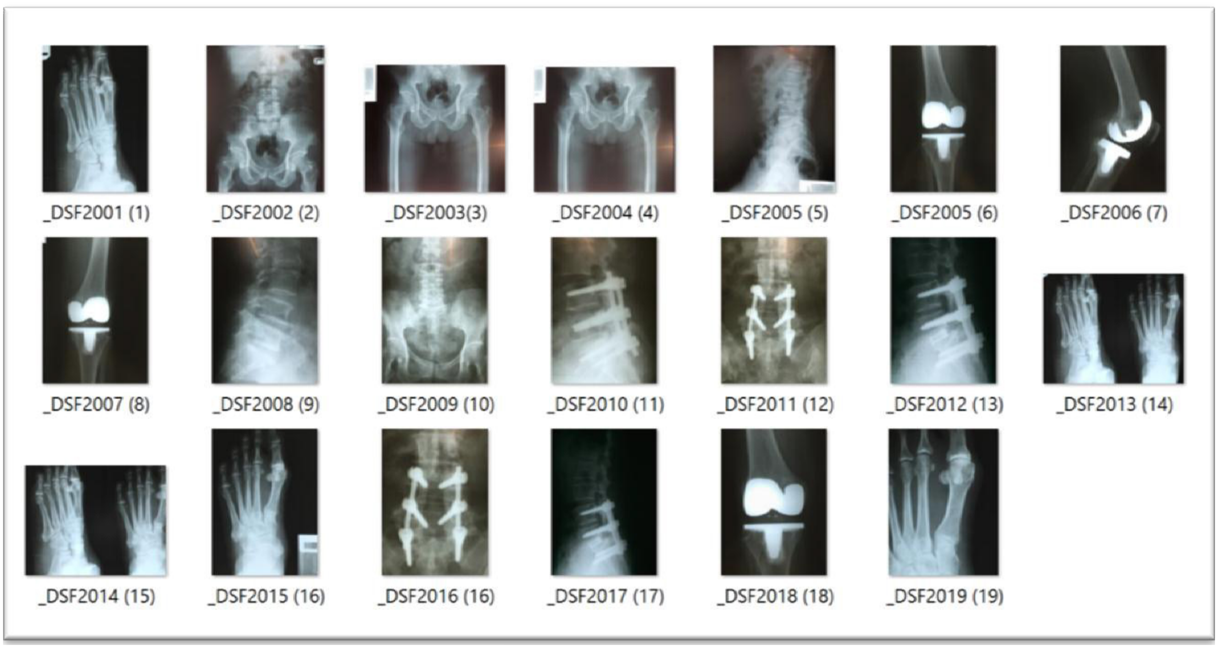

Figure 1 Raw images used in this study

The three hash functions that were used in this study were SHA-256, MAC Using AES-128-CBC (Key size 32), and HMAC Using SHA-256. For the encryption algorithms, this study used AES-256, DES, 3DES, RC4 and Blowfish. The RC4 algorithm represents the symmetric stream cypher technique. The rest were block cipher technique. The AES-256 represents the bigger bits to encrypt. The Blowfish represents various bits (38-448) by default 128 bits. DES represent 64 bits and 3DES represents 256 bits as AES-256.

All the image files were copied into two group. The first group is called "control group". The three hash functions were applied to all images. The hash values were recorded. The second (observation) group was processed by five encryption algorithms for each image and then three hash functions were applied. The hash values were recorded. **(Figure 2)** This study observed the avalanche effect of hash value before encryption against after encryption which was calculated by using the following equation[16]:

$$\textit{Avalanche Effect (\%)} = \frac{\text{(Number of Changed Bits in Ciphertext)}}{\text{(Total Number of Bits in Ciphertext)}} \times 100$$

The homebrew visual basic program was written to compare the avalanche effect on the hash value form control group against the encrypt group.

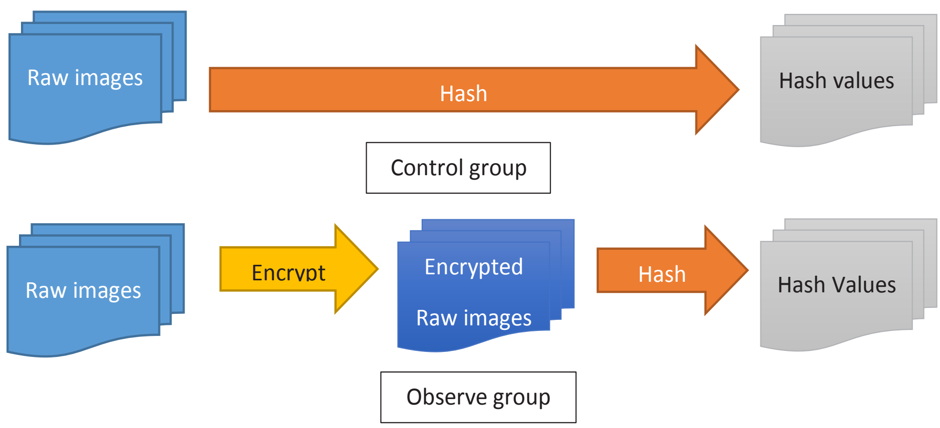

Figure 2 Process in each groups

The R Project for Statistical Computing program version 3.2.2 17 was used in this study. All the results had to test for normal distribution of the sample size. The one-way Anova with paired wise comparison of mean was used to test the analysis of the variance.

Results

The results of the study are shown in the tables below. The details of the results are in the appendix. Table 1 displays the sample of the results of three hash function algorithms of the control images. Table 2 displays the sample of the result of three hash function algorithms of the RC4 encrypted images. Table 3 shows the average avalanche effect between observed groups against control groups. The maximum average avalanche effect was the HMAC-SHA256 with 3DES encrypted image. The least avalanche effect was the CMAC-SHA256 with 3DES encrypted image. The range of the avalanche effect was 0.874612995 - 0.916771863 times. Shapiro-Wilk normality test were applied with all the groups for normal distribution test. All groups were normal distribution.

ANOVA single factor was, then, selected to test the mean of three hash function groups of five encrypted algorithms. The hypothesis was that all the mean values of each hash function in the same encrypted algorithm image group were equal (H_0). The means of the 3 three hash function are not all equal is the H_1. This study showed that two groups have rejected the H_0 Hypothesis which was RC4 and 3DES encryption algorithm image groups.

Table 1 The sample result of control group after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118. RAF	ab7e6338c259441c354adb2fc1498c15dcdc10769 fa5c873ede804a21f82d522	47d5c9af70916531c23ea 4cafa89d186	ecee0c87e7a09fd488e2b84 ebeef561de208f8dea154 b8c7a2a2bf6020da64e2
_DSF2119. RAF	972a96b6f8ff71917f2eb6cdc2c01d7fac87655bff7 d378380320aba5c8d261a	d9a749b6949ded9f8836c 7e139e23608	0000af7593caedad1949 fae242d311990f1593e7e2 5699c58aaaf437fd57747c
_DSF2120. RAF	b4fc12085a6a4511e49726e80d87bdd246ee78a7b ed65b5064fc642a0d49ec6c	53d223d47855ab515578 8d601eaf9d99	5aacd7bcfd0bc4ab7e2869 cd3e13c2643ddad86d6 da5c73bf0a498ce1eed924f
_DSF2121. RAF	a689d6b0e3e6542cb09157dcac3638f8f9d98bd1cfac8fbbf-c04cd6137e4e9c5	3fafa3595f387c7090399 af0dded06d0	af9584424ed39bce548886511 03b73185c8c5e590d28dab bf4150b470032506f
_DSF2122. RAF	7c81b60987bd66e41d8ed2e7853ea07a709c9916c 8307086cc3d4bd60bf32888	5b8ed6e075b3104013a6 77ca3f0351ae	f9fc627d806649c5ae6 e62754252ba1171d7685c4 50e9fd049d3d3b44d363dd7
_DSF2123. RAF	5e1297a3ddea5dcd6bad002f4e8f428ab560fc3103 0eaed96c4914c7957e48bc	97e61858b9151ef2ddca3 9dcf2e0adfa	f2b481878c991f12c531165d 3296a09affe4ad151e633a ede27c488e5741077
_DSF2124. RAF	d2d3c66ce6e3c6e3523792bdaef11248a3d08ffed6 ad6ceaf-9857e93fabaf5ef	51b57e0f0e3e9db4a54c6 88158caf9fd	1508aa21fdde65959d7386b b79ca7d1839bdd4ab130ed ea689e72d7c7bfd1558

Table 2 The sample result of hash function (SHA-256, CMAC-SHA-256, and HMAC-SHA-256) of RC4 encrypted group.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118. RAF	5e73baa20c8dcda022b8f9b031878961e76dbdd-e176760f603670e017461e811	d6e1db0067ec71375fd6 b8d89e297065	1b35db58ed35b380bda12 ccb558ae4d60ba9905c324a d88cb55331febd3ec0c3
_DSF2119. RAF	cd102375fa2e38b454cb4f2d453db26d08774297565a bc0d5bd0ed5e6d91fc46	375efb3fab4ea3052145960 147b9d3fa	95e39ddad2733246785c bfb4e6dbddca30a811264cc52 dfeb2101c1dabc5f440
_DSF2120. RAF	9f9d08015b8badf67765662e1bede658aa69b3e044be d3b8e18930a7fccffdb3	6a4e6cda2d66317fad3e392 fa3f5e2ed	bd5817f1e928534b3067805 f2ab2cc082f734173b8f0a76d 600078ad5c583cf3
_DSF2121. RAF	cdb9a1a3c00aa635e89b39508be31cb20dc9aed165e7b071 d5994c80dca0a197	13ea443fd8e8911d2490970 305cb98aa	d3f6d17d8e4cbf0403af5a898 aee902d5783732fed35d4a51 b38e5f76897983c
_DSF2121. RAF	91359fb96b1d97917d493223ab28f2275e1010d18423b118 b340 d8d3d5b8e094	8668b671dc519a663e67 b83c2766a15a	3a6ec57cca002ed6e4cc903838 acfd5acf4b45e2714a48ba6be c4744c3a629db
_DSF2123. RAF	3b30f6afc984729940a6cf1b19b2182ee8418362f01cd60f cd7c2df3f70d3c27	927606b4c4035ca083 e41079f88addfd	edd3950a9ab7facb899479095f4 e8871b0d5f84ace0718e2283 f0c266395ce5b
_DSF2124. RAF	f7c6e8e7a618f28cadd17909a164594d401d252bd3592bb 521b0f8ca17937780	0108c30200d6e7edfe73f917 ce982813	0673fee638af0bcf7e2d528d 6dde3f1a5a72090ba3bab85 deb810622a4856374

Table 3 The average result of Avalanche effect after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function for each image encryption algorithms against hash function of the control groups. (value in % must multiply with 100)

Encrypted	SHA-256	CMAC-SHA256	HMAC-SHA256
RC4	0.905901	0.880805	0.905901111
AES	0.901444784	0.885448905	0.905653174
BF	0.900694242	0.880804947	0.897864984
DES	0.907801	0.885448905	0.8921696
3DES	0.9062295	0.874612995	0.916771863

Figure 3 shows the results of ANOVA single factor with paired wise comparison of the mean test. According to the results, the mean of avalanche effect of HMAC-SHA256 VS. CMAC-SHA256 and SHA_256 VS. CMAC-SHA256 hash function of the RC4 encrypted image group were statistically unequal. There was no statistical difference in the mean of avalanche effect of SHA-256 vs. HMAC-SHA256 hash function of RC4 encrypted image group. **Figure 4** shows the results of ANOVA single factor with paired wise comparison of mean test. According to the result, the mean avalanche effect of HMAC-SHA256 VS. CMAC-SHA256 and SHA_256 VS. CMAC-SHA256 hash function of the 3DES encrypted image group are statistically unequal. There is no statistical difference in the mean of avalanche effect of SHA-256 VS. HMAC-SHA256 hash function of 3DES encrypted image group.

```
Fit: aov(formula = DIFF ~ TYPE, data = Dataset)

Linear Hypotheses:
                            Estimate Std. Error t value Pr(>|t|)
HMAC-SHA256 - CMAC-SHA256 == 0 0.025096   0.009919    2.53   0.0377 *
SHA-256 - CMAC-SHA256 == 0     0.025096   0.009919    2.53   0.0376 *
SHA-256 - HMAC-SHA256 == 0     0.000000   0.009919    0.00   1.0000
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
(Adjusted p values reported -- single-step method)
```

Figure 3 ANOVA single factor of the avalanche effect of the three hash functions of the RC4 encrypted image group

```
Fit: aov(formula = DIFF ~ TYPE, data = Dataset)

Linear Hypotheses:
                            Estimate Std. Error t value Pr(>|t|)
HMAC-SHA256 - CMAC-SHA256 == 0 0.025096   0.009919    2.53   0.0377 *
SHA-256 - CMAC-SHA256 == 0     0.025096   0.009919    2.53   0.0376 *
SHA-256 - HMAC-SHA256 == 0     0.000000   0.009919    0.00   1.0000
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
(Adjusted p values reported -- single-step method)
```

Figure 4 ANOVA single factor of the avalanche effect of the three hash functions of the 3DES encrypted image group.

Discussion

The Avalanche effect in this study shows the difference of mean by statistical significance in the RC4 and 3DES encryption algorithm group but the rest are statistically equal. The RC4 is the stream cipher technique compared to 3DES which is the block cypher technique. However, the results show that CMAC-SHA256 show statistical significance on the mean of the avalanche effect when compared to SHA-256 and HMAC-SHA256 hash function algorithms. The mean of the avalanche effect of the CMAC-SHA256 is the lowest among the same encrypted algorithm group. It may be from AES-128 key which was included in this hash function. The RC4 encryption algorithms are vulnerable to many treats, rendering it insecure (18). 3DES encrypted image with HMAC-SHA256 had shown the best performance in avalanche effect and meet the security demanded.[12] All the results also show the large amount of avalanche effect in all encryption and hash functions. The average avalanche effect is more than 87%. This mean with encryption algorithms can exaggerate the delusion effect of hash function.

The hash function value of the encrypted image may be used for image integrity check and also the encryption algorithm makes the image secure as a result. The security of the encryption algorithm is the major concern and the collision resistance of the hash function is the desired feature. Using a combination of these processes may be useful for the image storing procedure. According to this study, the combined selection of 3DES algorithm with HMAC-SHA256 may be the solution.

Conclusion

The encryption technique can exaggerate the avalanche effect from hash function. This technique may improve the collision resistance performance and security. The encrypted image should have enough security and integrity checking should have a collision resistant property. The combination of two processes may improve the image storing security. This study shows the use of HMAC-SHA256 with 3DES encryption algorithm is the best combination in avalanche effect aspect.

References

1. Bellare M. Chapter 4: Symmetric Encryption. CSE 207 Course Notes [Internet]. 2012;1–33. Available from: http://cseweb.ucsd.edu/~mihir/cse207/index.html
2. Radhadevi P, Kalpana P. Secure Image Encryption Using Aes. 2012;115–7.
3. Sajid M, Khizrai Q, Bodkhe PST. Image Encryption using Different Techniques for High Security Transmission over a Network. 2014;2(4).
4. Roe M. Performance of Symmetric Ciphers and One-Way Hash Functions. Fast Softw Encryption, Cambridge Secur Work Cambridge, UK, December 9-11, 1993, Proc. 1993;809:83–9.
5. Cryptanalysis of MD5 and SHA: Time for a New Standard [Internet]. Available from: https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.html
6. Kumar A, Tiwari N, Patidar, Ganesh Agrawal, Nitin Tarmakar S. Effective Implementation and Avalanche Effect of AES. Int J Secur Priv Trust Manag. 2013;3(3):1–4.
7. Jakubiuk V. Implementation and Performance Analysis of Hash Functions and Collision Resolutions. 2012;
8. Masram R, Shahare V, Abraham J, Moona R. Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features. Int J Netw Secur Its Appl. 2014;6(4):43–52.
9. Soediono B. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). J Chem Inf Model. 1989;53(December 1993):160.
10. Devi TAM, Sabitha S. Symmetric Key Cryptography on Images in AES Algorithm and Hiding Data Losslessly. 2012;2(4):2–5.
11. DES [Internet]. Available from: https://en.wikipedia.org/wiki/Data_Encryption_Standard
12. 3DES [Internet]. Available from: https://en.wikipedia.org/wiki/Triple_DES
13. SHA-1 [Internet]. Available from: https://en.wikipedia.org/wiki/SHA-1
14. SHA-256 [Internet]. Available from: http://www.movable-type.co.uk/scripts/sha256.html
15. Anova [Internet]. Available from: http://www.biostathandbook.com/onewayanova.html
16. Patidar, Ganesh Agrawal, Nitin Tarmakar S. A block based Encryption Model to improve Avalanche Effect for data Security. Int J Sci Res Publ. 2013;3(1): 1–4.
17. R program [Internet]. Available from: https://www.r-project.org/
18. Prohibiting RC4 Cipher Suites [Internet]. Available from: https://tools.ietf.org/pdf/rfc7465.pdf

Appendix

Table 1 Control group after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	ab7e6338c259441c354adb2fc1498c15dcdc10769fa5c873ede804a21f82d522	47d5c9af70916531c23ea4cafa89d186	ecee0c87e7a09fd488e2b84ebeef561de208f8dea154b8c7a2a2bf6020da64e2
_DSF2119.RAF	972a96b6f8ff71917f2eb6cdc2c01d7fac87655bff7d378380320aba5c8d261a	d9a749b6949ded9f8836c7e139e23608	0000af7593caedad1949fae242d311990f1593e7e25699c58aaaf437fd57747c
_DSF2120.RAF	b4fc12085a6a4511e49726e80d87bdd246ee78a7bed65b5064fc642a0d49ec6c	53d223d47855ab5155788d601eaf9d99	5aacd7bcfd0bc4ab7e2869cd3e13c2643ddad86d6da5c73bf0a498ce1eed924f
_DSF2121.RAF	a689d6b0e3e6542cb09157dcac3638f8f9d98bd1cfac8fbbfc04cd6137e4e9c5	3fafa3595f387c7090399af0dded06d0	af9584424ed39bce54888651103b73185c8c5e590d28dabbf4150b470032506f
_DSF2122.RAF	7c81b60987bd66e41d8ed2e7853ea07a709c9916c8307086cc3d4bd60bf32888	5b8ed6e075b3104013a677ca3f0351ae	f9fc627d806649c5ae6e62754252ba1171d7685c450e9fd049d3d3b44d363dd7
_DSF2123.RAF	5e1297a3ddea5dcd6bad002f4e8f428ab560fc31030eaed96c4914c7957e48bc	97e61858b9151ef2ddca39dcf2e0adfa	f2b481878c991f12c531165d3296a109affe4ad151e633aede27c488e5741077
_DSF2124.RAF	d2d3c66ce6e3c6e3523792bdaef11248a3d08ffed6ad6ceaf9857e93fabaf5ef	51b57e0f0e3e9db4a54c688158caf9fd	1508aa21fdde65959d7386bb79ca7d1839bdd4ab130edea689e72d7c7bfd1558
_DSF2125.RAF	6842da7e7c382e96509df0310688c18cbfa85ee34d38a55973b262d84cfc72e2	70dbaedec33b6566e7dd94bcc74566b2	85ee644782633d24aeee5ddf39bb44edf8f24fd39c3a380d886917b8f32248c
_DSF2126.RAF	352c0264d9d999a5b3930b7b4ac233b462142b8a53e34bdb921fbe200c3e734f	830943111db4f2e91b67f55145eca649	0ad5a2bff7c620ac464f46cc969cf0ccd0fdb65cb57c2b3584c239c29d9ba6fe
_DSF2127.RAF	d51e860a6ffc6883852a23fb7b6647629a99e1fd306df8c49e892be8b7278039	f941e5c8c31dd5b90f80fc0dd03928a7	f9700125e331eab92c7db78d5d439931039d31d63278f2484d43bf8531b99491
_DSF2128.RAF	11327f81161e4a7236cc532d99e61e45d2dc7b75b71670f54bf07d08dbdf8d39	18cfceb28c6c46a146dab960a3185799	958455f433ce9db33da21cefd0d56e25e770910c07a3eca10a5d8f60eb494ed3
_DSF2129.RAF	8c1e5f8953fd2cd7df10292913165f4832782e73f9ca60aa903f601730ededd8	72831b3de69459e146e4cc45c5a6a3b7	1842cd7f3995f8e3969b3fa106160689dfd372e70b3a5364dd767d20cff9d7d1
_DSF2130.RAF	e56e1dabe25de94fdcdb759446d2186fae1fd297afd1311b1439b35aaecb9f80	056ec67de349bc33c655125ad9d425fc	cb65b586d9f3dece07d08a00168971f5f48ce6e532992188604c7d0d0c2bcb3e
_DSF2131.RAF	d54109a8b8a5ccd04c7dd4b48c79ef53dd32d581665507e10dfafcfe67d97a9a	4d94676bfbeb8015bff501d49eb542b5	135b188d8afd27cdc1c03dd71cc77c6fb465db0015cfa3abcf10f83147cf725c
_DSF2132.RAF	b9052ac36c20825986aec0abc81b47d4d742eb99d7c547dcbd5a7bf436ae8c6a	83ed6806c2c73f8d3e3758ab630ae815	8bee986a9c228bf2008cf60e951b7d1c9ce67e43259416998d0bcda299cf3704
_DSF2133.RAF	fb03471c41e58d7c679cadd702bb061f5ee3ff98d1064321451315ce6add8478	ae064d24bb080741ed25fb820640f9b0	a4a62de2f7b61088d7fc3022f7bc904a365c2c3ac1f56745c96974c782579b2b
_DSF2134.RAF	04b20def6c902f7aeffb38805e2950554c1d778dabccf346285a70217c774f22	846cb4fb6fffedf46fe627dcfefed584	9222adc9c3e1dc51ea0978061840da6dfc2b0bce91338bf6e88e0fa760e7ef1b
_DSF2135.RAF	bb47fda3eb14864f21e3a18f150a9ac21b359e5561ea93810a60c2e76a04660a	9655b6a40e4fb8028f7841a0cf1ff50c	d59ae991aa57670d3b32c8feac88a5e58310e7a9f59f580b25faa929ef8c7d5e
_DSF2136.RAF	50d980174f346c6057c8cfbee458ee5623b0944eac126042d3b05b1cd9b6b756	8147c10f4278bab0a509def240d418e8	ecf43df0ef8f1c91576ed8bd1ea57e13204b8e474fa79a64a10a6800022c7f8

Table 2 RC4 encryption after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	5e73baa20c8dcda022b8f9b031878961e76dbdde176760f603670e017461e811	d6e1db0067ec71375fd6b8d89e297065	1b35db58ed35b380bda12ccb558ae4d60ba9905c324ad88cb55331febd3ec0c3
_DSF2119.RAF	cd102375fa2e38b454cb4f2d453db26d08774297565abc0d5bd0ed5e6d91fc46	375efb3fab4ea3052145960147b9d3fa	95e39ddad2733246785cbfb4e6dbddca30a811264cc52dfeb2101c1dabc5f440
_DSF2120.RAF	9f9d08015b8badf67765662e1bede658aa69b3e044bed3b8e18930a7fccffdb3	6a4e6cda2d66317fad3e392fa3f5e2ed	bd5817f1e928534b3067805f2ab2cc082f734173b8f0a76d600078ad5c583cf3
_DSF2121.RAF	cdb9a1a3c00aa635e89b39508be31cb20dc9aed165e7b071d5994c80dca0a197	13ea443fd8e8911d2490970305cb98aa	d3f6d17d8e4cbf0403af5a898aee902d5783732fed35d4a51b38e5f76897983c
_DSF2122.RAF	91359fb96b1d97917d493223ab28f2275e1010d18423b118b340d8d3d5b8e094	8668b671dc519a663e67b83c2766a15a	3a6ec57cca002ed6e4cc903838acfd5acf4b45e2714a48ba6bec4744c3a629db
_DSF2123.RAF	3b30f6afc984729940a6cf1b19b2182ee8418362f01cd60fcd7c2df3f70d3c27	927606b4c4035ca083e41079f88addfd	edd3950a9ab7facb899479095f4e8871b0d5f84ace0718e2283f0c266395ce5b
_DSF2124.RAF	f7c6e8e7a618f28cadd17909a164594d401d252bd3592bb521b0f8ca17937780	0108c30200d6e7edfe73f917ce982813	0673fee638af0bcf7e2d528d6dde3f1a5a72090ba3bab85deb810622a4856374
_DSF2125.RAF	eae2a2b97e928ee72068682a21e5ca5d8613914fdeb6609fb36f81c77efdd4a4	6a32792290ad50e3e84671df8eaa42c8	b50f64b06398d0291f7516ef6b6431d87f01dc58018813c84ebf9eb6327be1e1
_DSF2126.RAF	3e1141b32f40b7b63a6240a239ecb75311bdbc3c83401111ead3c1511637efed	00fa6d9c875fb0284bbde353a0372ff0	952cfaff976b51bc615342a52c1e153d37a916f3d340231c365ec74923257f9e
_DSF2127.RAF	8c2a7252c1504ec3d1a22eb5b98d17536451468bfc16b427a20c4c1091f283e1	828460bf5b29f68484bd850cb83e5612	6264387a641b5c618ce294d44ffa9b44ed114c2fdf185b51fadec7415a561cab
_DSF2128.RAF	64f3080bd57f229e2112c977860b7fff1ae2bf75b2f30856248070c96c1f74de	1f70e593a619e9b45c322eecf04b7af5	34be89a3d38d227d4670fe86de61b71cc02daa4f4aa5d76047293a6907631608
_DSF2129.RAF	98f6e17d6b9c731f7efbc4bfdc7630e0ef02e352a4fc29bcaf38d7829918faa0	7d07ad66ad7a5241433ef18f57c43ef9	7a7a3f81afa8e843691a983d4018b1542863ecd7e9ca3cf8f73dae3f5771894c
_DSF2130.RAF	8680786fcea9dc0eb877429f9d667bb43bdb5a87d2213ec4b12f9e416024fadd	9cecdebdcbbd28aa83729cb028d984a7	6f3d3c7d0983bc466a7562f50abeb19a12be35285aa86c74da3598020bb7cec9
_DSF2131.RAF	5b83087dc76c13d0086de54db1eff4ca21e0f061a8eb4c857d900f75d4c1d76c	b196faa9560d85077962e84747d12fc1	9c1fc7c58233d31180193e3cda238ea5d3f2a8b9dc6b9661a5828e3d5046701e
_DSF2132.RAF	81f3fa09b7384d25eb7a619569cb869f5420096da8c6b2e21e411d7c6974f519	2fdef94e75b82d77ca94fbfe2fe96fe	d5f183d4f942437c1387ff16bce5b044fef76f85be58ba43d30ce137161dea82
_DSF2133.RAF	f541e737b13ec9c76409dda02552a9a61498a35c2f3cb7a6229a963c708f575f	7661d509af0ce2fe3428348f75ae50a0	a3ad7a773b6c69f4b4c3d65ba232dedecf0dd9e729e02372278bf3081a02df94
_DSF2134.RAF	23ab9beb4bc8c30eb75868cc25ebec05f3c731ce273ec2c609f515a6e48540d1	eb1456e8f4b53a291de144f204cefd92	bf7b26d346a801fbd6404a734e13de936576ca64ed4175c8b7db98d155e68b1f
_DSF2135.RAF	d6ee7e54ec341e92e81713f05d62aceb81a8c535bd1055d4a7929e1b7aded2a1	b8f999b0a086950406678d271b3ebbaa	915811607911a623ea309039ac40e8c10f27b695293ae39a5e55586e2eb10417
_DSF2136.RAF	aacf1568ff6b91dcde36b7cfb91d20db9bbb82f55671c4d2c5d88114ec606ee6	265333629fc16ccaf2af4d02d75b78cf	a89a4dc7d57d9d6746263b4760090e237094d56a78c2f4a271f82634eafad788

Table 3 AES-256 encryption after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	9c1b48f5e77dd4f9e6cdde81a776b77fa7aede024630cdb0f5252c364a105cf5	06de52cb87a7cf1bf1cd204660dd34b6	14d9c1688921141 4ef17bf065bc9c6df9b64ede090363d6df0cfade21a7a13d3
_DSF2119.RAF	0a3fdaf3747baf8c9c83c1c52551e91088db279e2cfd10b7a0d22533a160fd7a	9072624022a7e1b0e13748ea654a6309	08a582e4ac1ba6047803cb696c1bd566ff8be43b91027c346f7b495277e5dd16
_DSF2120.RAF	c2d7f97b3fad0780ac43b14ecfd199d7cd68f99a24a884f1ac8a161dd6424b4b	c3b1f9150ab77b9cc520b2cc7d9a5403	7fbafc697126e28a27de1b1441adf4bd0e692940cfe9bb275bfb6546fc247e29
_DSF2121.RAF	78caf19a9dfc39a3dcd8a7c7fcd5ebd224dc74164a7323c887a6229ba6370eb6	1c6e3df3b30018334bfcd2fc3d6135b7	5e7bdfcedd701051bbf0d6387f1c336df36f3979edc87231e7f91865ddd632ef
_DSF2122.RAF	342b45a1da377f7402a1ef11a8b68b5a8edefe0b8a1b9cf429e20809f0f58613	4ea1d28cb706e4132be577d334a33298	a794a5259db2f7887528147888c6ecefd11b3a265d894ddf42f5bc0447da4155
_DSF2123.RAF	cad0608ab35551e48fcd730c37f87b01a8b69fb1accdb28dcfd712a0cd6e67a1	ab68dd46e57bed8e532b9fa9112fad9c	c0ad67b884442cb1bcafdfd0069db103fdec0f1e17062e947aad0cfaabf0bcd9
_DSF2124.RAF	95d02ecffa96468313364a0f1693d6160d158153e19d799679a27a21bfffee54	0fc4965d2b73be0747b69e778568a4ab	afb32f2e6369257c98b6971d0f642f76c7ae7b50bd7d3808ffec8751675475ea
_DSF2125.RAF	c8e8123f076b8c783701e41da5b1413405d04518afd4641aa540996440a78229	2a0c483ab7a64367c8a8bd7370859243	94e22b6e84ce14a9e9568f1ee66af88ee21fb426ebb1ba55c8b533733088c25d
_DSF2126.RAF	aa1d7f60b3e829dd0f8f9b06b860e19eb9a3a90961d5f3f5cbce05d222f25dc3	7143758d59ad42d358d2a2106283c274	87b0a5402e5bc25443e715c5b77370e23ed892286fb158be2b41c116319249a1
_DSF2127.RAF	915c7f61270cebb00536f3bcf1ce47838473d6c058ef5ade9bb97c354cbfd8eb	8456a45658b2d9de618b1289abb474f5	c5d0e2566914f7eb56c3aa6878b816969c81d48f7a7dba592e2753e644072fa5
_DSF2128.RAF	12062e9f3565a078929d10a4af084a9700fd18974055f2852f4daa75760e2709	8e05233429e4694ac2ae182c4f3bcfcc	7d902ae307e0c9c214958e513061143d9b1128810507e56f330c8057fd1f99aa
_DSF2129.RAF	b690538ffbb8cbaeaae7d80b3bc8ee6956e504044e58fdc3af1eebe110869345	aa2addc112032246a1f43297851f07be	9303f961c21520432d0ef2582a1aed6ca751098b2e5f52dd79a1e048d125411a
_DSF2130.RAF	aeaeb002f853f855e21d39c2573645aa1a081562c952c41269499926082f2676	d26f13a1da1f684092c0b46ac9c0bb8d	3a4bf05557df15d3486d0c3c971cf2a4f91ae9ec2c939fcfea9a11e788086006
_DSF2131.RAF	46104eb94aa9b4df89b4a457409709e31a0a49c68b02401dbdbb2e45dc60b6df	f1374e715d8f9ad8124029b026eb0111	1150bcc54461e58fb6904adc14f5460c475d36993306af1d1be9646b6e947e0d
_DSF2132.RAF	e537f5fc47205e73647ab7890f0ce7302ec24c0b76a09b524858fc59de226863	1ea58434ebcc16ee375ada194af4899a	4dc805cb22ff6da21aca332aa6d7906e0c2b975d4aeb5e18c4e21cad42233b3a
_DSF2133.RAF	30d2cc3ebc1b7e8ef549402c3a59997f8b706795cba38ad96b3d4912d6617b0e	d06e58c730242d163e3f83bfb2f43894	97c95bbd84d1c056d3232e66a8ea8e9c9856a70d2f019532870b36671f1585e1
_DSF2134.RAF	1b90cc8745d77113342e51cc6b099bae506d8d46e830fc26b059ae2864e97b62	9eae6cbed7236776a456e40b09dc4525	9e326feb251f9b278916dda14c3c5d94b42e1af9fe5f3c0cce301b1d4819a1f3
_DSF2135.RAF	1cdede85d856e2ee25545e1ba70aead5c1117544e06e6211840129c5e53fd748	c7bf2c08c76fd9d8a0f82a1d11fa1f50	848897cd37a07f0543506c15ebe97e9f8a19eebc5e5de7ed4bfa3388fedae355
_DSF2136.RAF	8cc8440f8ab967b1f9f275f505e855b616340bb92d639439388b277a2a15c3e9	6383a6a3b6264358448fcc7caf4228a1	73b15e69e47a6905a1286090456e5c00aed805ed511c7e67e81bc9a5bf64ead4

Table 4 BF encryption after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	a85e127e3c1633d970c7763eadeba2f62d5764ae7bfc8d7c4b1281fddfab0be3	c5a4fe7a85d14fe6f6ac940801f0e732	14de5e3132bbbdc55da735bbcd969f260be1764aad80af30637b0a48cb13dcda
_DSF2119.RAF	d722cab31418bc3bfd383a845ea553fbe8c906e4a0e587b55f7baf87f5b9c903	ecaaa96a3eba9360869e4f3bfad6ec6a	945dc15e83428bdcea07ceb33fe0b763c6d65f86b646dee9907968da93e17de6
_DSF2120.RAF	279f13da08cfbdc660b14a72c28b0ab5f46838ff95027d36eebec30212fd688b	210b02797a623170be16e2b59410e968	aa424b001a577ba05dd1e8f54ef5ec4b537c591c2d0657a8d0f45546675299c2
_DSF2121.RAF	34a355ac491a35a215519b52366d13fb4376b52bce88587d53040da42bbf57ba	d505d160c2d4adb3872e61a688396478	735676bb16bf5a60c0bb4c54f1fba7634d7691e15c38b9f120ed2866cc32ba19
_DSF2122.RAF	bdaabd5618abfdb4708477301a3dd7fea85a09580ef619e47a97506aa58541d2	84702e1a78ce831e820e6cfadaa4463e	dbd3e99a0764b1649b7563619a7f30b17a4f8e05e65f87824c5be107e4647f02
_DSF2123.RAF	29865eb69cd75dc6bb304d1732a96002467a1fc7a8a1e61fb644740352dc080c	2bff86108f6e6c7c2fa0a0bb9a574145	37e97e44043c9238f48d4634dcab83fdf265c08e01deaac008e553c5a2e0c125
_DSF2124.RAF	7184d27fb2d16992ae497d940f3f404ba44f41f010cfc2cd1780474f88b36b5c	5a186394c4df53364fb829883fe29a70	f9c81df4707068b6d80912967d127dcceec16c46f8fe83d958538ab67540f1c6
_DSF2125.RAF	306d75657988b35a8c1d4f3077be4b1831797636c318783b41476e8a069e973f	5a186394c4df53364fb829883fe29a70	e508ed1313c3ff8602e99c9f7460afed79bbe4df3ea115172a3618152a3e8da0
_DSF2126.RAF	fbe8c04a5efc71a88bf142a5152fa5e1b29872dedf8b82f689d6a9f74339e094	8703f8f8f3342785acea315d2e1e3114	0251dfe5b6de38be153f5c1ce04abac640f445fa14a219d29c8f3017c988fcfa
_DSF2127.RAF	9fff6e7299f35de996a454acd8b329b9af55c4648d1c0edd0da9383e3361ac47	5ae0b85d50df18cedd7b5c010e275d4f	8c7ad9f6e82c0bac8614053fff5ae59de7f3520912ebe0a5a656ee31d6954479
_DSF2128.RAF	e3479790faa037410766f11017456dc59b8df4ccaef70755233b9c4d85ed8de3	412cdd8777094e7c5d0486a28cb5cac8	a94c788e672540473915 2f8bcf25f571764f3f91803810025aaea42f3fbc4e46
_DSF2129.RAF	e972035cd250d0dbc8ec2a92e24b517a9ff594fcc4c98c952c072fbcadc9ca0f	f3531895a895514163e792a2b71b3762	7d53db3169668ac669fa4f3f2618272adbcd546429e201903c95616f053f9a4d
_DSF2130.RAF	b82626188d92553c65afdb0862c4a0c89a1261b1fe563159b1c7e0a7dcae74f0	0b51740b3b5d1ea525f7f47a2f05cca7	7d88f1710896cc12666efe3264c7d83c7a2374c1204009bedf24842c362c8215
_DSF2131.RAF	d2831ddb11d73b63478e06cfefc713fdf14a15b514aa170005c7830129772a42	f59d129e5782000e88a90d2b76ea14ab	c552906909f143a3740db44fe34956d06caad4893a6da92f12cf909243894262
_DSF2132.RAF	b42a1cbb7a1ce494b49fb0d553daaedddc5b3159551ecfec43d4e01af082d201	54ed040b63a9c2051ae167e7a5d111e9	7a709a782dd2b4a6f4129408ea2422a8c1ba1933a1e001458e266c97a2140057
_DSF2133.RAF	1ef20984b5bf48b92c27634cca747f877170457adf49d01c2a5f0ed5bd86fe27	e4c9f3d45b108c100a913fa97a120d0b	772877a87d839737e8b94fb2393e3c09674740ccf6647e7237900d5a6e2e92c2
_DSF2134.RAF	e9a2948736d9111e5839bdaa34eea7aa5f28113e8a487ef20d8a19b43478eb89	0ab5a338b62d718f93c566b556d84c38	8c3d6e43dc76c4c97518aab0edf77ea8924c71618e8d4f0234723685e956c76a
_DSF2135.RAF	1e45855b3b7c0f08949ad5bcf55706b52df43b4d603cb89823dfd30576e3f009	c5a3b0ecb1a44f68ecb49ef002c8c35f	bf355567a6718f77fbd2805ed3c6083bc339b05e928398fea8ca8ea236de8542
_DSF2136.RAF	4b684989f9354f95e465cf004f741611c733e979257d7c1a871cf0fc931913bf	63a3d8b7f7e966d00b222630ffca6ca0	c4a10421078056ccf084faec129decf37c1ede75d188c8a764a528b86949fe26

Table 5 DES encryption after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	a236c053e94eb5e71927d128d4499bd6de209c2f7860ffb5245e3633066c91ee	5a7f2a8544ae6d2ffce4a77e70a1bf46	a92ffa73ea9097b44085eed3360a1778f993a935e333b511e254f02f5973e130
_DSF2119.RAF	11122f101a0c0e2434ced337132b70cd9d6be9bf359e65d1932d5e36bf88835f	184df6e1adbcc971099e3376a53c0698	3551f25a3256144d82aecc2f214dff7be1019a3527f65998ad2814dfd8edf3fa
_DSF2120.RAF	3c38523b412692d0ff12094cbb65582a82b2727682e8d86e2675da5c4d526382	af60383c25e3c3be20c94207558d6788	0692b3087b2d1dc8f7bef6cb4c178f98e3b2ea1f81cfe408f71833bb6f2886d0
_DSF2121.RAF	f6b9990cd50e8f9cf550f33638c168b66ce0d08a3a6b35ef155aec099ccd0049	5e64c31f87f421dc55f0d40cbff599e0	4e5b559146f2e3fe73681c5f4f05dd912e6ce38cb0c756b859dd9b7201bf912e
_DSF2122.RAF	188bc664bdfad608cabfeaa8f38ea876212e5dd8e89f308d65c83121301fa81b	8bcc5677edbf8b1d079650b3b6963d9c	aa9d9fcce6ac722a381bfcce689baee242f390cee228b84b147d81a3b62abb33
_DSF2123.RAF	2cde62ede0dbee06ca23f62ebe931ccf127ddea0db2f883128113f096625f81d	37e9cc48c1694bfc3eb824a8e3b3ca7e	82504c7ca6a8e37b27225a87b9bc95ba4bd47b7c8b9551be2fb76fed7732fb41
_DSF2124.RAF	07531ba941853dc715cc2b223fa3fbbd1e0073808dca7a9845ee17f3716d9538	d64f7db64746e022dda17dcf26f83cf2	4048e3da7fff7e396e173cc747c2706e34b9e1879118cbd9d9678791adca17d18
_DSF2125.RAF	cb36d5ddfb000a2067730457555be61a9e72abf7b37e76e78610afe4f2a98710	b2902996349da376bc098fd4b40d77c1	a960352fbe113ec321aa5f2dc6dffe0a8fb17f9e7eaa30ddaca7611a0a7dadcc
_DSF2126.RAF	a2a8238278a3bee4b154dd8b6563c2953a7c211f3e7ae23e5a1c14781241126c	7a681df7f84bceb0651d589b7f9ae0fb	ecac788b3b0605f54d3fed4052245fffe2f12db67732cabf8955579a05cdb205
_DSF2127.RAF	f5b2e3a6f5dbea83d7a2011056397da66eea76ff48f4af69c364402f25b7bba6	764bc44cc2eb1e2ae92c56ce806118f2	2bfded15d584cb3dc8a9c45e6341703b51d04855ebb1712d552da9ae3ae40960
_DSF2128.RAF	162c6fe77a2e65812d1638d74bf31d308eab5cb8c50b2dc 9247c3d626fadc8d4	48139b36b024175c6dce98806602d52b	a1911a0a4c08f20c7c7d0fbc4754470622c7c9c1f0dec1a0095df6c550d9e9e6
_DSF2129.RAF	adbcc2f0ad4b631bd7b1087a3ee504b00a2be8fc57e73a23414d8f92e657e84f	0f6663aa4cf0a54e49f9850664bcf321	f12967a05af62810a634daa14ee7072661420ce7ee8121d2ec43e75e1b65d930
_DSF2130.RAF	458ebef127c118188095f26f515694c26cde35fcd99aeb06f510195d6f514546	267584d533a8572d521658cd4e9617eb	4ca2356e1d2064951b1c5ab47d0a650b4fd2651199f65adaa30eb71c70b32609
_DSF2131.RAF	9a2509727c65d5d22b6e3ed1e39f84ec7df0d723ad4e7c57fedbe56f03d071fa	2185b5be8ce5af67dcfd7875d4f357ae	fc9d87508fa4b62940c00cde873e4038a65957d021ff413b66c53efe05d20bb8
_DSF2132.RAF	a46367608bdd766c18d3f1d300cd7e86881bfe6db0b8ab9437a581aa71175f7a	a726cea2b113abc291576a9032704380	47c9b3e9815541b023fde9c51037650e237e5ed6a8bfd99f013273555479e63c
_DSF2133.RAF	ba0655faafb949dacfcf2b2bd38b40186147babb9c6a3f09da70f5f1ef098890	303273353a4086e86df447d59f0f6b9b	bad1e8e84b8920ff296139d3b1d8c0da30a40993649b7746cdf2b30207172a6a
_DSF2134.RAF	f93f1c007812dce3a5f86ed8d20bbcdd334fc13a7913ea60536c9970b44fc7cf	f1543435553603a1ba9896a837a62e25	c027385817813813 64e70c547e158507c6d41c247a140dd8bdfe2950be540afa
_DSF2135.RAF	8977808b638c594203712f816a472b8761bacc9f7243555eb9e3095cce3bd041	5d6769ecc98e421d96f5d6bcc31ede3c	49002fa2cbfe373338078e3176a9803b6e50eac92aa36dbdd95bdd0e81674fc9
_DSF2136.RAF	71d304a29286d7fd7fc3fea37ceebcd4d29483f0894ebc4006728e03f3287b29	b007ddf29ceccbfd14575265a253afc9	dcb5b37fd5036843a42c5cc5ac2bb1e20f6db44aec0f862f8b93bf9d1692d0d9

Table 6 3DES encryption after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function.

File name	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	e6f7d0c0f4aef33cd21e84dbbdb1c20fc81a45298fda6fd9587f10ea1b530d59	e57b6d032c804a88cc3b3952640311ee	62316cd04603e80bc50f89a3ed496be24f51566ca6faf33c6a9e2c73e2b8284f
_DSF2119.RAF	28349a4113b121e9012443b5a784adcf1c77c9079b6bf93a1bf80b00aa324a62	f1748c8c71f610cb22b22e9111c028f1	6beecb2b0f2e8b8eeb501498ee796b16b634df745e399bcace5649a851569533
_DSF2120.RAF	f70c1f92474f1200ce617d519f4572b4eea06be0cad6e8985f812b8020297dbe	633c86110ca65e51a63ec74f58b29259	1f746db7efd2c1ce59f20165353504bc314538fecacd156df176ddd215e63a6
_DSF2121.RAF	67d296c27ce5f9ddefd4cd0728e3a06a214d65ab5993e0c8a53fe71ffc69da1e	0393d219d7999fd1391bec5f70b4973a	d37dc443b192b9fe37788fdd51b64c950c7529543751371d77f9bd1138af3a30
_DSF2122.RAF	b00bc5559d4b108d42c4015d56f0720c66b9df2820fa45dcb53b295dc7c64d8d	b77c9d18286708011b394d8a55336b41	37d8d829691af2f40d2671813d3590a1ab69695a3d01a93065d7b6d8a578e3b3
_DSF2123.RAF	b26b2bb3871077ecf4ddde81726d242ebf8eb5a48859b7e70504ce1e165e8163	533024932b12cb2b2d0cec55676929a5	89a3de209f39d739de724a0448bd1f76f6941e00d769102fe8ad4b03cd666570
_DSF2124.RAF	de7855ea015cf1bca8e5b7e802dc65699e1039cf5e5fa4d976f3fdf9cf4f55d7	8220c009756fd70f9f39eaff0fa8ca17	38a5a2b0cbf6f937554a07189fcbcfd4d10c365a5fc9952c1d3734120fc08275
_DSF2125.RAF	fd9526ffb61c000edf6cd4fce4022f1ff6d75fa68d3d4085f575786593a6090c	1d534f712d03ad25a6f585b0ca40fb51	049e260e414bda9a52a9c4677d3b35c23e136cbd17aeac45896fb014ca07b0d3
_DSF2126.RAF	d0b2e8bc30a230bb78594e47c25ed5522a17b459b1b80578d8099423a1182a46	cbef121302a53f96ab8dd7ad7ce91413	455501332d1e653a95ab91d6abc61772beeca92f5cae5856af944fea0f806f86
_DSF2127.RAF	83ffa4ef5e630c3488ec37939b429e737388a9da84eb9412ce69039309d1f082	c1d7179da3a07d7a217d63c7f53c8b32	dbe4507e8656d7ed9d2018b8d791d5462e301d019a13b632835361039eec68bb
_DSF2128.RAF	2e7f6285b71f6de9bcd283176914b43b8af1d3b145b971722aa7c52a7ee0c869	54f92413458639380e767a7b9ffea7eb	f2d58fdbccf113577d4f79bd9df59f24d86de3ab7a928dde818cdf69ec3ca858
_DSF2129.RAF	10306c3441f9fadb226f71e4987e8c39769c5ee7bc952d4e6951aa48730af5a2	f7b038277d3dc1b6eeb7c9d626ab7841	f394d4c3e5f2ebbe5f42062b47a1e242939f0daa5a8ecc3f32475289ab094112
_DSF2130.RAF	e8bb03a9753766d76083a078bd325353242038bc5489afd8be83be5b3d50f443	5ad51ca2875bdd4c654d6dd33239d0f2	d8c6d082fef53b42746669568f1f379fe8fc3636d361dd27e1477ada3dd31f8a
_DSF2131.RAF	4f06bdd9ca437c22150c06d81b679b696e4f7a4f0b0c635eaae945e25a74c96e	746287b3e6fd432c8feca9bbab030cb7	ab82ea4a3997e417aa19b1be893589e007c29114c601c91245715a620a12c36f
_DSF2132.RAF	2851c2c5e0265ea0035711dddc3338e3a0ceabd8d80f978e80ed85e26a29e788	55b4fdfd9dd63fb7a19da94f43ee340d	acce56b1d81a85c57aa7c38b33d4996eaa85f455b3e104a36cd5487976c1eb9d
_DSF2133.RAF	7991146ac7c6cd97a5393344adb69661a9528af372b5f1dc379bf0219dbd3970	89f87f9660c3ed8849456a3af63312f0	2c99fe89bf3f841ef39d9561885d262ceff156cb16ae0d9eacdb4db4456afc42
_DSF2134.RAF	7215ca361c43ff30c3e299824821af0867013ef1bbf1591a5d783005fc02ee32	596f83a90759806ca765cf329e50f867	2335fd1ef2678a2815bf774a488c2310d03362a10c4bf6bf61e1c6b4b1eb03c4
_DSF2135.RAF	5f429d315e6ef075cd3c648f42e0e95069f06c3d46300b0b17cce9717db79ff9	cc538cc2a7f715e4edca0d813ca7e104	e8099ea8de4df8e3f7151ba99a04b3251eb938601ef2a7ccc9211fd53e105518
_DSF2136.RAF	b598b3d771bd589b9dcb80d65dcda30c56444b5b9590c00bcea62946013e23f0	a17938603aee77a93bb3e42eb5d89e42	6e2a2882c49bb4ed03e9de7c5d5db0c0ad835e3edcaaa3c4f8b11ff7ed5e4efc

Table 7 Avalanche effect after SHA-256, CMAC-SHA-256, and HMAC-SHA-256 hash function for each encrypted images against control group (value in % must multiply with 100).

	RC4			AES-256			BF			DES			3DES		
	SHA-256	CMAC-SHA256	HMAC-SHA256	SHA-256	CMAC-SHA256	HMAC-SHA256	SHA-256	CMAC-SHA256	HMAC-SHA256	SHA-256	CMAC-SHA256	HMAC-SHA256	SHA-256	CMAC-SHA256	HMAC-SHA256
_DSF2118.RAF	0.9090909	0.8823529	0.9393939	0.9242424	0.8823529	0.9090909	0.909091	0.8823529	0.939394	0.878788	0.8529412	0.878788	0.924242	0.8529412	0.939394
_DSF2119.RAF	0.9242424	0.9117647	0.9393939	0.8939394	0.8235294	0.9393939	0.909091	0.8529412	0.924242	0.939394	0.8823529	0.893939	0.848485	0.9117647	0.924242
_DSF2120.RAF	0.9242424	0.9117647	0.8787879	0.9393939	0.8529412	0.969697	0.924242	0.9117647	0.848485	0.924242	0.9411765	0.924242	0.893939	0.7941176	0.848485
_DSF2121.RAF	0.8939394	0.8823529	0.8787879	0.9242424	0.8823529	0.8787879	0.878788	0.9411765	0.893939	0.909091	0.8823529	0.848485	0.939394	0.9117647	0.863636
_DSF2122.RAF	0.8939394	0.8823529	0.9090909	0.9242424	0.7941176	0.8787879	0.893939	0.8529412	0.893939	0.818182	0.8235294	0.969697	0.939394	0.8529412	0.878788
_DSF2123.RAF	0.9393939	0.7941176	0.969697	0.8939394	0.8823529	0.8939394	0.848485	0.9411765	0.939394	0.924242	0.8235294	0.924242	0.909091	0.8823529	0.939394
_DSF2124.RAF	0.9090909	0.8529412	0.9242424	0.8484849	0.9411765	0.8939394	0.893939	0.8823529	0.863636	0.909091	0.8823529	0.863636	0.924242	0.9117647	0.924242
_DSF2125.RAF	0.8636364	0.9117647	0.8787879	0.9090909	0.8823529	0.8787879	0.878788	0.8823529	0.878788	0.954545	0.9117647	0.893939	0.954545	0.8529412	0.909091
_DSF2126.RAF	0.9242424	0.8823529	0.8636364	0.9242424	0.9117647	0.8939394	0.924242	0.8235294	0.848485	0.909091	0.9411765	0.893939	0.924242	0.8529412	0.954545
_DSF2127.RAF	0.9090909	0.8823529	0.9242424	0.8636364	0.8823529	0.9393939	0.939394	0.8823529	0.909091	0.893393	0.8235294	0.909091	0.893939	0.8823529	0.954545
_DSF2128.RAF	0.8787879	0.9117647	0.9090909	0.9090909	0.9411765	0.9090909	0.909091	0.9117647	0.893939	0.893939	0.8823529	0.893939	0.878788	0.9117647	0.878788
_DSF2129.RAF	0.9393939	0.8235294	0.8787879	0.8970588	0.8529412	0.9090909	0.882353	0.7647059	0.893939	0.911765	0.8823529	0.848485	0.897059	0.8823529	0.954545
_DSF2130.RAF	0.9090909	0.8823529	0.8787879	0.9090909	0.8529412	0.9090909	0.909091	0.8823529	0.954545	0.924242	0.9117647	0.939394	0.893939	0.9117647	0.878788
_DSF2131.RAF	0.8787879	0.8823529	0.9090909	0.8939394	0.9411765	0.9411765	0.878788	0.8529412	0.852941	0.833333	0.8823529	0.838235	0.954545	0.8529412	0.941177
_DSF2132.RAF	0.9242424	0.9411765	0.9090909	0.8787879	0.8823529	0.8571429	0.878788	0.8529412	0.842857	0.954545	0.9117647	0.885714	0.893939	0.8529412	0.871429
_DSF2133.RAF	0.8939394	0.8235294	0.9393939	0.9393939	0.9411765	0.9090909	0.954545	0.8823529	0.939394	0.893939	0.9117647	0.818182	0.893939	0.8529412	0.969697
_DSF2134.RAF	0.8939394	0.8823529	0.9242424	0.8636364	0.8823529	0.9242424	0.924242	0.9411765	0.969697	0.954545	0.9117647	0.924242	0.848485	0.8823529	0.909091
_DSF2135.RAF	0.9090909	0.9117647	0.9242424	0.8939394	0.8823529	0.8636364	0.893939	0.8823529	0.863636	0.924242	0.8529412	0.893939	0.909091	0.8823529	0.954545
_DSF2136.RAF	0.8939394	0.8823529	0.8333333	0.8970588	0.9117647	0.9090909	0.882353	0.9117647	0.909091	0.897059	0.9117647	0.909091	0.897059	0.8823529	0.924242