برخورد در کدگذاری فاز تصادفی دوبل

برخورد یک وضعیت است که زمانی اتفاق می افتد که دو یا چند ورودی مجزا به یک سیستم امنیتی خروجی های یکسان را تولید می کنند، که در برخی از برنامه های امنیتی نامطلوب است. این امر به ویژه برای برنامه های کاربردی از واترمارکینگ و تصدیق هویت صحیح است. در این نسخه ما یک مطالعه از ویژگی کدگذاری برخورد فاز تصادفی دوبل را ارائه می دهیم. ما نشان می دهیم که می توان برخوردهای دیگری از متن رمزی، علامت واترمارک جاسازی شده در در تصویر میزبان با استفاده از تکنیک های بازیابی فاز ایجاد نمود.

کلمات کلیدی: کدگذاری فاز تصادفی دوبل، برخورد، تحلیل رمزگذاری، بازیابی فاز

۱. مقدمه

اصطلاح برخورد اشاره به یک رویداد که در آن دو یا تعداد بیشتر بدنه برخورد می کنند و یا در فیزیک گرد هم می آیند. با این حال، در شرایط امنیت اطلاعات، این وضعیتی است که هنگامی رخ می دهد که دو یا تعداد بیشتر ورودی مجزا به یک سیستم امنیتی تولید خروجی یکسان می کنند. این برخورد در برخی از برنامه های امنیتی نامطلوب است. مثلا در مورد تابع هش، که رشته ای با اندازه ثابت و منحصر به فرد را (کد هش) از هر ورودی تولید می کند و به طور گسترده ای در یکپارچگی و تکنیک های تایید رمز عبور داده ها استفاده می شود. اگر یک مهاجم یک ورودی را یابد که یک کد هش یکسان با یک کد قانونی تولید می کند، او می تواند به سیستم به عنوان یک کاربر قانونی دسترسی پیدا کند. به طور مشابه، هر سیستم واترمارکینگ همچنین باید دارای خاصیت مقاومت در برابر برخورد باشد. در غیر این صورت، تشخیص مالکیت هر ویژگی واتر مارک شده غیر ممکن است.

کدگذاری فاز تصادفی دوبل (DRPE) برای رمزنگاری نوری، پنهان نمودن تصویر و واترمارکینگ استفاده می شود [۱-۳]. اخیراً مطالعات متعددی وجود داشته که نشان می دهد سیستم های کدگذاری فاز تصادفی در برابر انتخاب متن رمزی شده، پیام متنی انتخاب شده و حملات پیام متنی آسیب پذیر هستند [۴-۸]. با این حال، تا به امروز هیچ

مطالعه ای در مورد مقاومت در برابر برخورد برای این روش وجود ندارد. پس انگیزه ما در این مقاله بررسی ویژگی برخورد DRPE است.

۲. الگوریتم برخورد

در DRPE، یک تصویر ورودی و یا واترمارک، f(x,y) در نویز ثابت سفید کد گذاری می شود، به عنوان مثال، متن رمزی g(x,y)، با استفاده از ۲ توزیع آماری فاز تصادفی مستقل واقع در سیستم F۴ در صفحه های ورودی و فوریه. بنابراین برای پنهان نمودن تصویر و برنامه های کاربردی واترمارکینگ، g(x,y) در تصویر میزبان برای ارائه یک تصویر واترمارک شده جاسازی می شود ۲]،۳]. تصویر میزبان دارای اثر زیادی روی تحلیل ما نیست، به دلیل استدلال مندرج در پاراگراف بعدی. در اینجا ما فقط روی کدگذاری فاز در بحث های خود تمرکز می کنیم. فرایند کدگذاری می تواند به صورت ریاضی در [۱] بیان شود

$$g(x,y) = \mathcal{F}\{\mathcal{F}\{f(x,y)\exp[j\phi(x,y)]\}\exp[j\psi(u,v)]\}, \qquad (1)$$

که در آن (x,y) و (u,v) به ترتیب مختصات فضایی و حوزه های فوریه، ، و نماد نشان دهنده تبدیل فوریه است. دو توزیع فاز به صورت تصادفی یا فقط مورد دوم در مورد ورودی واقعی، به عنوان کلید امنیتی سیستم عمل می کنند. به طور کلی برای بازیابی واترمارک، f(x,y) به طور مستقیم از متن رمزی g(x,y) بدون استفاده از این دو کلید مشکل است. هدف از تحلیل ارائه شده در [۴-۸] بازیابی بخشی یا همه، برای اطلاعات این کلیدها با مورد پیشین است، اما دانش ناقص پیام متنی و / یا متن رمزی، و در نهایت بازیابی هر پیام متنی رمزگذاری شده با استفاده از همان کلید تنظیم صورت می گیرد. برخورد، از سوی دیگر، شامل پیدا کردن یکی دیگر از مجموعه های کلید می شود که متفاوتی برای g(x,y) یکسان، متن رمزی f(x,y) رمزنگاری می کند. اگر چنین برخورد وجود داشته باشد، کاربر غیر قانونی می تواند مالکیت هرگونه دارایی را، ادعا کند از جمله هنر دیجیتال، واترمارک شده با g(x,y) که به صورت قانونی متعلق به شخص دیگری است.

برای پرداختن به این مشکل، ما فرض کنیم که کاربر غیر قانونی می تواند به مجموعه کامل متن رمزی دسترسی داشته باشد $g(x,y)$ ؛ این فرض معقول است چرا که در برخی از سیستم های واترمارکینگ مبتنی بر کدگذاری فاز تصادفی، $g(x,y)$ به طور مستقیم به تصویر میزبان برای به دست آوردن تصویر واترمارک شده اضافه می شود [۲]. اگر تصویر میزبان در برخی از برنامه های کاربردی در دسترس باشد [۹]، استخراج متن رمزی آسان است. در مواردی که تصویر میزبان و $g(x,y)$ جدا نیستند، این کار روی عملکرد الگوریتم زیر تاثیر نمی گذارد از اینرو طیف تصویر واترمارک شده می تواند به عنوان محدودیت در صفحه فوریه مورد استفاده قرار گیرد. بنابراین ما می توانیم تصویر میزبان را در بحث های خود را نادیده بگیریم. با $g(x,y)$ می توان تبدیل فوریه کامل مختلط آن را نیز به دست آورد:

(۲)

در این صورت مشکل برخورد می تواند بدین صورت اظهار شود: یافتن تصویر واقعی، و دو توزیع فاز و به طوری که معادله ی زیر معتبر باشد:

(۳)

یک کاربر غیر قانونی که در نظر دارد به عنوان یک کاربر قانونی عمل کند دارای انعطاف پذیری کامل در انتخاب یک تصویر واقعی از خود تعریف شده به عنوان برخورد ورودی است. هنگامی که چنین تصویر ورودی انتخاب شده باشد، دامنه در هر دو طرف معادله (۳) تعیین می شود. بنابراین این هدف به پیدا کردن فاز یا به طور معادل با توجه به دو اندازه گیری شدت، به ترتیب، در فضایی و صفحه فوریه کاهش می یابد. این مشکل می تواند با استفاده از الگوریتم تبدیل فوریه تکراری (IFT) حل شود [۱۰]. با فرض اینکه الگوریتم به تکرار Kام رسیده است ، و فاز بازیابی شده است می توان برآورد تصویر را در حوزه مکانی شکل داد. بنابراین تکرار موفقیت شامل مراحل زیر می شود:

(I تبدیل فوریه برآورد تصویر

(۴)

(II) جایگزینی پیمانه طیف حاصل توسط برای تشکیل برآورد تبدیل فوریه:

(II) فوریه معکوس، دامنه مختلط مدوله شده را به حوزه فضایی دوباره تبدیل می کند:

(۶)

(IV) جایگزینی پیمانه حاصل با

(۷)

به طور کلی، هیچ راه حل تحلیلی برای معادله (۳)وجود ندارد. ، اما راه حل های امکانپذیر همیشه [۱۰] وجود دارد. فرآیند تکرار شونده فوق تا زمانی تکرار می شود که معیار های همگرا برآورده شوند. به طور معمول عامل همگرا می تواند به عنوان میانگین مربع خطا (MSE) و یا ضریب همبستگی بین انتخاب شود. از آنجا که IFT الگوریتم اساسا یک الگوریتم کاهش خطا است، بنابراین تعیین همگرایی ها با ردیابی MSE و تست اینکه که آیا کوچکتر از یک مقدار آستانه از پیش تعریف شده است یا نه معقول و منطقی است.

وقتی که فرآیند تکرار شونده پس از N تکرار همگرا می شود، توزیف فاز از لحاظ عددی به دست آمده ظاهرا یکی از کلیدهای مورد انتظار است. با توجه به توضیحات در مرحله II، طیف فوریه باید محدودیت حوزه فوریه را برآورده سازد یعنی با این حال جزء فاز نمی تواند اینگونه باشد، بنابراین باید یک مرحله اضافی به این مورد برای ارضای محدودیت فاز اضافه شود. این اختلاف فاز می تواند به عنوان کلید در نظر گرفته شود.

۳. شبیه سازی کامپیوتری

ما شبیه سازی کامپیوتری را برای نشان دادن تحلیل نظری موارد فوق انجام می دهیم. تصویری که ما به عنوان واترمارک قانونی استفاده می کنیم تصویر "ایلین" از ۵۱۲ *۵۱۲ پیکسل در اندازه است، که می تواند در پایگاه داده [USC-SIPI ۱۱] یافت شود. پیرو معادله (۱)، محاسبه متن رمزی مربوط .g(x,y) با استفاده از دو ماسک فاز تصادفی و آسان است که توزیع های نویز سفید هستند و در متن نشان داده نشده اند. پس از اینکه برخورد انتخاب

شود، به عنوان مثال تصویر "لنا" [۱۱]، الگوریتم بالا می تواند استفاده شود. معیارهای همگرایی استفاده شده در شبیه سازی MSE با مقدار آستانه برای مثال برابر با .۰۰۱۵ است.

این الگوریتم با ۱۰۰ تکرار همگرا می شود. رفتار همگرایی در مقیاس لگاریتم منحنی با نشانه های مثلثی در شکل. ۱ نشان داده می شود. در واقع می توان دید که منحنی خطا بسیار سریع در چند تکرار اول کاهش می یابد ، و بنابراین بسیار هموارتر می شود اما کاهش آن همچنان حفظ می شود. این رفتار معمولی همگرایی برای الگوریتم کاهش خطا است [۱۰]. دو توزیع فاز تصادفی و بازیابی می شوند. به طور کلی، این دو توزیع از کلید های فاز قانونی متفاوت هستند. اختلاف فاز بین کلیدهای فاز قانونی و غیر قانونی و همچنین از نیز دارای ویژگی نویز تصادفی است.

در شبیه سازی ما، مقادیر مورد انتظارو ۸۳,۱۳۶ و ۳,۱۳۶۹ رادیان هستند، که نزدیک به π هستند و انحرافات استاندارد از هر دو ۱,۸۱۴۴یافت شد. به منظور نشان دادن واضح کاراکترهای تصادفی برای این نقشه های فاز، نمودار هیستوگرام آنها در شکل ۲ رسم نمودیم که نشان می دهد آنها توزیع هایی متحد بین $[۰,۲\pi]$ هستند. حتی اگر کلیدهای فاز غیر قانونی بازیابی شده به میزان قابل توجهی از موارد قانونی متفاوت باشد، می توان آنها را برای رمزگشایی تصویر انتخاب شده از $g(x,y)$ با کیفیت بالا استفاده نمود همانطور که در شکل ۳نشان داده شده است. MSE ، بین آن و "لنا" ۰,۰۰۱۵ و ضریب همبستگی نرمال شده بین آنها ۰,۹۹۱۱ است.

شکل ۱. رفتار همگرایی الگوریتم در مقیاس لگاریتم. MSE با استفاده از فرمول محاسبه می شود که در آن و محدودیت فضایی و تصویر بازیابی شده در تکرار kام و M*M اندازه تصویر است. همان طور که در متن توضیح داده شده، این طرح رفتار الگوریتم را برای هر دو دامنه کد گذاری و طرح ورودی فاز کد گذاری شده را نشان می دهد.

توجه داشته باشید که ما هیچ محدودیتی را در انتخاب تصویر برخورد واقع ،مقدار دهی اولیه الگوریتم یا طیف متن رمزی در بحث فوق و شبیه سازی تحمیل نمی کنیم. خاصیت همگرایی برای تمام برنامه های کاربردی از الگوریتم کاهش خطا همانطور که در [۱۰] ذکر شده برقرار است. این بدان معنی است که کاربر غیر قانونی دارای انعطاف پذیری زیادی در انتخاب است و همیشه می تواند دو کلید امکان پذیر و را از تصویر انتخاب شده و طیف فوریه به

دست آمده بازیابی نماید. بنابراین این الگوریتم بدون در نظر گرفتن طیف فوریه آنها، g(x,y)، در مورد رمز نگاری، و یا جمع وزنی برای یک g(x,y)+a یک تصویر میزبان، در مورد واترمارکینگ استفاده شده همگرا می شود. این ویژگی نیز منتج به مشکلات بسیار جدی در برنامه های کاربردی عملی می شود: هر کسی که می تواند به g(x,y) دسترسی داشته باشد؛ میتواند مالکیت خود را از هر چیزی که توسط g(x,y)واترمارک شده ادعا کند. زمانی که بسیاری از ادعاهای مالکیت از یک تصویر یکسان شامل خاص و زوج کلیدی فاز صورت گیرد، تبدیل به یک مشکل برای انجام ارزیابی های فنی در مورد حقوق دارایی می شود.

شکل ۲. نمودار هیستوگرام اختلاف فاز بین کلیدهای فاز قانونی و غیر قانونی:

شکل ۳. تصویر برخورد با کیفیت بالا بازیابی شده در شبیه سازی

حتی اگر واترمارک f(x,y) از پیش در تابع فاز کد گذاری شود، هنوز برای پیدا کردن برخورد ممکن است هر چند چنین پیش پردازشی در افزایش دشواری و تحلیل همچنین در مورد رمزنگاری مفید است، [۱۲]. در این مورد، فقط نیاز به تغییر محدودیت در حوزه فضایی (مرحله IV در الگوریتم) برای دامنه واحد وجود دارد. در این مطالعه ۲ توزیع تصادفی شبیه به فاز و همیشه می توانند یافت شوند به طوری که الگوریتم همگرا شود [۱۰]. در شکل ۱ نشان داده شده است که این الگوریتم با توجه به دامنه واحد برای محدودیت های فضایی در این مورد سریعتر همگرا می شود. بنابراین می تواند به صورت جمع از هر گونه تصویر برخورد و توزیع شبه تصادفی نوشته شود یعنی . این و در حال حاضر به عنوان کلید غیر قانونی به کار گرفته می شوند.

۴. نتیجه

توابع هش رمزنگاری برای احراز هویت (امضای دیجیتال به عنوان واترمارک ها)، یکپارچگی پیام، و تایید رمز عبور استفاده می شود. برخوردها در پنین توابع خطرات امنیتی جدی را در برخواهد داشت. در حالی که هیچ خطر برخوردی با DRPE وجود ندارد هنگامی که کلید بخشی از ورودی نیست (بر اساس تعریف، زیرا روش رمز نگاری متقارن نمی باشد)، ما نشان داده ایم که DRPE برخوردها را هنگامی می پذیرد که کلید به عنوان متغیر ورودی در نظر گرفته شود و DRPE به عنوان یک تابع هش رمزنگاری مورد استفاده قرار گیرد. اگر چه شرایط ایده آل برای رمزنگاری لازم است [۱۴]، این خاصیت نشان دهنده ضعفی است که نیاز به تعمیر و DRPE استفاده شده برای احراز هویت با این روش دارد.

وجود این برخوردها ناشی از ماهیت خطی سیستم و روش رمزگذاری فاز است. اگر چه معرفی سیستم تشخیص اضافی در حوزه فوریه ممکن است برای فراهم نمودن یک واسطه در ارزیابی مالکیت مفید باشد [۴،۱۳] زمانی که لازم است، برخی از اطلاعات در مورد طیف جاسازی شده در تصویر واترمارک شده نیاز می شود. با این حال این اضافی اطلاعات ممکن است توسط کاربر غیر قانونی برای تجزیه و تحلیل واترمارک و کلیدها مورد استفاده قرار گیرند.

قدردانی

G. Situ از Humboldt Foundation von Alexander سپاسگزاری می نماید. T. Naughton از پشتیبانی یاران از کمیسیون اروپا از ماری کوری از برنامه چارچوب ۶ سپاسگزاری می کند. این کار توسط Science for Science, Foundation Ireland, Enterprise Ireland and the Irish Research Council Engineering and Technology حمایت شده است.